



FORCEPOINT

Sidewinder

Product Guide

8.3.2P03 and later

Revision C

© 2017 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
Raytheon is a registered trademark of Raytheon Company.
All other trademarks used in this document are the property of their respective owners.

Published 2017

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Forcepoint. Every effort has been made to ensure the accuracy of this manual. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Table of contents

Preface	9
Conventions.....	9
Find product documentation.....	9
1 Introduction to Sidewinder	11
Features of Sidewinder.....	11
Networking elements.....	11
How to control access.....	14
Protection from attacks.....	15
Encrypted content inspection.....	16
Global Threat Intelligence.....	16
Planning and setup	19
2 Planning	21
Planning your setup.....	21
Integration Checklist.....	37
Quick Start Wizard Response Form.....	38
3 Installation and configuration	41
Requirements.....	41
Install the Management Tools.....	42
Configure Sidewinder.....	43
Configure using other methods.....	46
4 Startup	53
What the Admin Console does.....	53
Activating the license.....	56
Complete post-setup tasks.....	61
Policy	65
5 Policy overview	67
Types of rules.....	67
What access control rules do.....	68
Logic of SSL rules.....	73
Interaction between rule types.....	80
Rule order.....	81
6 Network objects and time periods	85
Types of network objects.....	85
Manage network objects.....	86
Manage netgroup membership.....	89
Manage time periods.....	90
7 Identity validation	93
Validating users and user groups.....	93

Passive identity validation.....	94
Active identity validation.....	95
Users and user groups.....	106
8 Content inspection.....	113
Methods of content inspection.....	113
Configure IPS inspection.....	114
Configuring virus scanning.....	125
How McAfee Global Threat Intelligence works.....	128
Benefits of SmartFilter.....	136
9 McAfee EIA.....	147
How McAfee EIA works.....	147
Benefits of McAfee EIA.....	149
Understanding file reputation in the firewall audit.....	150
Configure certificates.....	152
Configure McAfee EIA settings on Sidewinder.....	156
View active hosts connected to Sidewinder.....	163
View related firewall audit.....	164
10 Applications.....	165
Using applications in policy.....	165
Manage applications.....	173
Manage application groups.....	175
Updating application signatures on an isolated network.....	177
11 Application Defenses.....	179
Understanding Application Defenses.....	179
How the Generic Application Defense profile works.....	182
Virus scanning.....	186
Managing Application Defense groups.....	188
Managing Application Defense profiles.....	191
12 Access control rules.....	197
Creating and managing access control rules.....	197
Configuring access control rules.....	197
Examine how access control rules overlap.....	204
Create access control rules and groups.....	207
Modify access control rules and groups.....	208
Arrange access control rules and groups.....	208
View access control rules and groups.....	209
Modify general settings.....	211
13 SSL rules.....	213
Configuring SSL rules.....	213
Duplicate an SSL rule.....	219
Modify SSL rules.....	219
Arrange SSL rules.....	220
View SSL rules.....	221
Configure which columns are displayed.....	222
14 Policy in action.....	223
Working with policy.....	223
Allowing a custom application.....	224

Allowing inbound access to internal servers.....	225
Allowing outbound web access.....	233
Allowing IPv6 network flows through the firewall.....	236
Configure IPv4-to-IPv6 translation for HTTP.....	239
Configure non-transparent HTTP.....	243
Controlling access based on user identity.....	246
Create an alternate policy.....	249
Creating SSL content inspection exemptions.....	250
Decrypting and inspecting SSH content.....	252
Deny access based on country of origin.....	257
Deny access to an application category.....	258
Discovering which applications are in use in a zone.....	260
Examine your policy using the Firewall Policy Report.....	262
Inspect and control inbound HTTPS.....	262
Inspect and control outbound SSL (including HTTPS).....	266
Create a rule to allow traceroute through the firewall.....	271
Create a SPAN policy.....	272

Monitoring.....277

15 Dashboard.....	279
What the dashboard monitors.....	279
Use the dashboard.....	280
16 Auditing.....	283
Importance of auditing.....	283
Viewing audit data.....	289
Filter audit data.....	296
Transferring audit records.....	307
Managing log files.....	309
Export audit data to syslog servers.....	315
17 Audit responses.....	317
Understanding attack and system responses.....	317
Managing attack responses.....	318
Managing system responses.....	324
Ignore network probe attempts.....	328
Enabling an SNMP trap.....	329
18 McAfee ePolicy Orchestrator integration.....	331
ePolicy Orchestrator and Sidewinder communication.....	331
Configure firewalls for ePolicy Orchestrator reporting.....	332
Troubleshoot Sidewinder to ePolicy Orchestrator communication.....	333
19 Network defenses.....	335
Viewing network defense information.....	335
Restore network defenses.....	337
Configure the TCP network defense.....	337
Configure the IP network defense.....	338
Configure the UDP network defense.....	339
Configure the ICMP network defense.....	339
Configure the ARP network defense.....	340

Configure the IPsec network defense.....	341
Configure the IPv6 network defense.....	342
20 SNMP.....	345
Your SNMP needs.....	345
Setting up an SNMP Agent.....	345
When to use the SNMP pass-through.....	359
Networking.....	361
21 IPv4 and IPv6 overview.....	363
Support for IPv4 and IPv6.....	363
Firewall IPv4 and IPv6 support by area.....	364
Access control rules and IPv6.....	367
22 Security zones.....	369
What isolates networks.....	369
Configuring zones.....	370
23 Interfaces and NICs.....	373
Attributes of a network interface.....	373
Manage interfaces.....	380
Manage NICs and NIC groups.....	392
Test connectivity for an interface or NIC.....	395
24 Quality of Service.....	397
Quality of Service and how it works.....	397
QoS scenarios.....	398
Configure Quality of Service.....	400
Enable DSCP pass-through.....	407
25 DHCP Relay.....	409
How DHCP Relay helps.....	409
Configure the DHCP Relay server.....	409
Create DHCP Relay rules.....	411
26 Routing.....	413
Routing protocols in firewall.....	413
Configuring static routes.....	414
Configuring dynamic routing server processing.....	419
What RIP does.....	420
How OSPF works.....	429
Concepts of OSPF IPv6.....	434
What BGP passes.....	437
Why the PIM-SM protocol is used.....	443
Dynamic routing in HA clusters.....	456
Troubleshooting dynamic routing issues.....	456
27 DNS (domain name system).....	459
Types of DNS modes.....	459
Configuring transparent DNS.....	460
Configuring firewall-hosted DNS.....	461
Reconfiguring DNS.....	477

DNS message logging.....	480
Configuring DNSSEC.....	480
28 Email.....	487
Email options.....	487
Set up and reconfigure email.....	492
Configuring advanced sendmail features.....	494
Managing mail queues.....	503
Managing email messages sent by firewall.....	506
29 VPN (virtual private networks).....	509
Benefits of the Sidewinder VPN solution.....	509
Plan your VPN.....	511
What VPN user interfaces help to do.....	520
Example VPN Scenarios.....	522
Create VPN policy.....	532
Maintenance.....	561
30 Administration management.....	563
Management options.....	563
Admin Console access management.....	565
Command line interface access management.....	567
31 General maintenance.....	575
Manage administrator accounts.....	575
Understanding time synchronization.....	578
Configure time synchronization.....	581
Configure network clocks.....	583
Configure firewall self-diagnostics.....	584
Enable hardware acceleration.....	586
Understanding software management.....	586
Update software.....	588
Shutdown options.....	596
Configure the firewall for UPS.....	598
Register the firewall with Control Center.....	599
Manage service updates.....	600
Editing files.....	601
Backing up and restoring the firewall configuration.....	606
Make the firewall FIPS 140-2 compliant.....	616
32 Certificate/key management.....	617
Managing certificates.....	617
Managing remote identities.....	633
Managing keys.....	634
33 High Availability.....	639
How High Availability works.....	639
HA configuration options.....	641
Configuring HA.....	644
Understanding the HA cluster tree structure.....	649
Managing an HA cluster.....	651





A Troubleshooting	663
Rules.....	663
Determine functioning of HA.....	672
Troubleshoot logon issues.....	676
Check network status.....	678
NTP.....	684
Startup.....	687
System status.....	690
Troubleshooting transparent (bridged) mode.....	692
Troubleshooting VPNs.....	692
Contacting technical support.....	692
B Re-installation and recovery options	695
Need for re-installation and recovery.....	695
Recovery options.....	696
Re-installing options.....	700
Re-install your firewall from the virtual CD.....	700
C Glossary	703
Index	707

Preface

This guide provides the information you need to work with your Forcepoint product.

Conventions

This guide uses these typographical conventions and icons.

<i>Book title, term, emphasis</i>	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
User input, code, message	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext	A link to a topic or to an external website.
	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Warning: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

On the Forcepoint support website, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product on the Forcepoint support website at <https://support.forcepoint.com>. There, you can access product documentation, Knowledge Base articles, downloads, cases, and contact information.

Introduction to Sidewinder

Contents

- [Features of Sidewinder](#) on page 11
- [Networking elements](#) on page 11
- [How to control access](#) on page 14
- [Protection from attacks](#) on page 15
- [Encrypted content inspection](#) on page 16
- [Global Threat Intelligence](#) on page 16

Forcepoint Sidewinder (Sidewinder) allows you to protect your network from unauthorized users and attackers, and to protect internal users as they access the Internet.

Features of Sidewinder

Sidewinder combines an application-layer firewall, user-based policy, IPsec VPN capabilities, SSL decryption, and McAfee® Global Threat Intelligence™ into one security appliance that is designed to offer centralized perimeter security.

These features provide powerful configuration options that allow you to control your users' access to almost any publicly available service on the Internet, while mitigating threats to your organization.

Sidewinder uses SecureOS, an enhanced UNIX operating system that employs Type Enforcement security technology. SecureOS removes the inherent security risks often found in a network application running on non-security focused commercial operating systems, resulting in superior network security.

Networking elements

These sections describe the networking features of Sidewinder.

Related concepts

[Zones](#) on page 12

[IPv4 and IPv6 support](#) on page 12

[DNS](#) on page 13

[VPN](#) on page 13

[Routing](#) on page 13

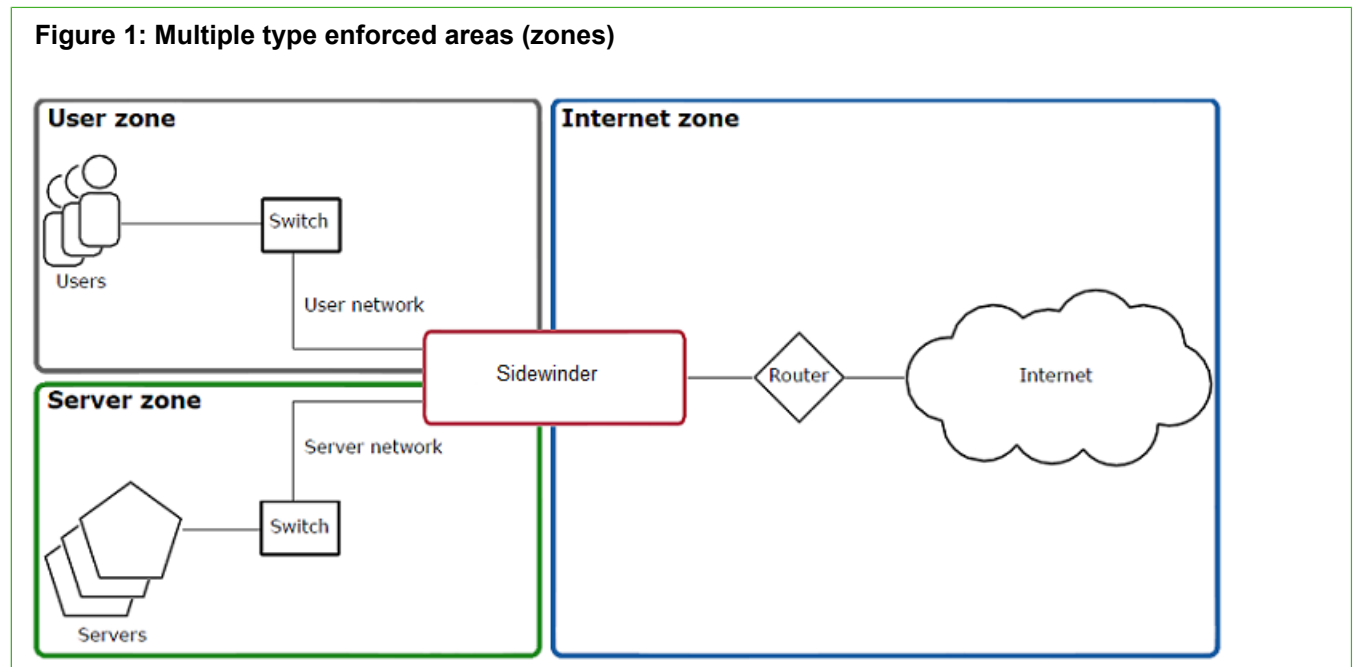
Zones

Zones are compartments that isolate networks with different security requirements from each other. *Zone* is a term that refers to a firewall network interface and all the systems it connects.

Zones allow you to assign policy to individual interfaces; firewall policy is enforced when traffic attempts to cross from one zone into another zone.

As an example of how zones are used, suppose your organization has two internal (protected) networks that need to be connected to the external network (Internet). Your corporate security policy requires that information flow is limited between the two internal networks. In this scenario, you would configure three zones for your Sidewinder, as shown in the following figure.

Figure 1: Multiple type enforced areas (zones)



To allow network traffic from one zone to another, create the appropriate access control rule.

Related concepts

[Configuring zones](#) on page 370

Related tasks

[Create or modify a zone](#) on page 370

[Create or modify a zone group](#) on page 371

[Delete a zone or zone group](#) on page 372

IPv4 and IPv6 support

Forcepoint Sidewinder supports both IPv4 and IPv6 addresses, allowing you to integrate with more networks. IPv6 support also gives you access to larger blocks of routable addresses.

The following connection types are supported:

- IPv4-to-IPv4

- IPv6-to-IPv6
- [non-transparent HTTP only] IPv4-to-IPv6



Note: An IPv4 host cannot connect directly to an IPv6 host or vice versa under any circumstances. (For HTTP IPv4-to-IPv6 translation, the firewall is acting as a proxy server, so there is no direct connection between source and destination.)

DNS

Sidewinder offers two main DNS modes, giving you the option of a simple firewall configuration that can be used with a separate DNS server, or a firewall-hosted DNS configuration that allows you to manage external DNS and gives you control of all DNS records.

- **Transparent DNS** — Transparent DNS is designed for simple DNS configurations. The DNS server is on a separate computer, and DNS requests are passed through the firewall. This mode is the default DNS configuration for a newly installed Sidewinder.
- **Firewall-hosted DNS** — Firewall-hosted DNS is a more complex DNS configuration that uses the integrated Sidewinder DNS server. In firewall-hosted DNS mode, DNS servers run directly on the firewall, so you do not need an extra computer. This places the DNS servers on a hardened operating system, preventing attacks against these servers from penetrating your network. Sidewinder uses Berkeley Internet Name Domain (BIND 9).

You can configure firewall-hosted DNS to use a single server or split servers.

- **Single server** — The hosted DNS server is not bound to any zone.
- **Split server** — Two DNS servers are hosted on the firewall, one bound to the external zone, and another for use by all internal zones. Internal network architecture is hidden in this configuration.

Routing

The firewall uses static and dynamic routes to integrate with your networks, and it can act as a default gateway for your network.

The firewall supports five dynamic routing protocols:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF) protocol
- OSPF IPv6 protocol
- Border Gateway Protocol (BGP)
- Protocol Independent Multicast - Sparse Mode (PIM-SM) protocol

VPN

You can provide secure access between protected and remote networks, or between protected networks and remote users, through the firewall Virtual Private Network (VPN).

You can provide secure access between protected and remote networks, or between protected networks and remote users, through the firewall Virtual Private Network (VPN). The firewall VPN uses the IPsec protocol suite, which provides secure data transmission across unsecured networks through an encryption and decryption process.

You can apply access control to VPNs using rules in the same way you do for physically connected networks.

How to control access

Access control rules determine what traffic is permitted through the firewall and what is denied.

Each rule requires an application, which identifies the type of traffic matched by the rule. An application can be as general as a protocol and port(s), or targeted at a particular web application using signature information.

McAfee AppPrism

McAfee® AppPrism™ provides the application discovery and control that allows you to monitor the applications running through your network, and to allow or deny them based on your policy.

You can use McAfee AppPrism to create policy that protects against specific threats and reduces bandwidth usage by restricting the use of non-business applications.

- **Application discovery** — When enabled, identifies which applications are traversing your network
- **Application control** — Allows you to determine which applications are allowed and denied

The burden of identifying an application's protocols and ports is placed on the firewall instead of the administrator. Use the provided applications, firewall applications, or create custom applications. Create access control rules based on individual applications, application groups, or application category filters that block all applications belonging to a specified category.

User-based policy

User-based policy allows you to tailor access rights to individual users and groups. Users and groups can be stored on the firewall or on separate servers such as Active Directory, LDAP, or RADIUS.

You can configure the firewall to validate user identity either passively or actively.

- *Passive identity validation* leverages the users and groups that are already configured in your organization's Microsoft Active Directory. User status information is monitored by the McAfee Logon Collector software and communicated to the firewall—the user is not prompted for authentication by the firewall.
- *Active identity validation* prompts a user to provide credentials. You can also configure an Active Passport so that an authenticated user's source IP address is cached, and subsequent connection attempts are not prompted for authentication.



Tip: You can also use McAfee® Endpoint Intelligence Agent (McAfee EIA) to collect user and connection information from Windows-based systems.

Protection from attacks

Sidewinder attack protection defends against attacks in both allowed and denied traffic.

The firewall has multiple layers of protection that work together to protect against known and unknown attacks. Some of these defenses occur automatically, and some of them must be configured. The following sections explain the different options.

Application Defenses

You can increase the protection provided by access control rules and SSL rules by using Application Defenses, which offer customizable protection at the application layer.

The defenses can be used to enforce Request for Comments (RFC) standards, enforce allowed parameters, and enable inspection methods, such as McAfee Global Threat Intelligence. Configurable parameters include headers, commands, versions, and file sizes. You can use these controls to deny any parameters that are not essential to your business needs and to minimize your network's attack surface; the fewer the number of parameters allowed into your network, the fewer parameters an attacker can use to attack.

Intrusion Prevention System

The Sidewinder Intrusion Prevention Service uses signature-based files to detect and prevent known network-based intrusion attacks, such as hacker-generated exploits and protocol anomalies.

IPS can be added to access control rules to inspect allowed, incoming traffic for these attacks as the traffic enters the firewall. If an attack is detected, the rule handles the attack according to the configured response. Response options range from completely ignoring the traffic to blackholing all traffic sent from the originating host. This attack protection is particularly valuable when you cannot minimize your attack surface because your organization requires services with known vulnerabilities.

Attack responses

Attack Responses can be configured to notify administrators when audit events are generated by suspicious traffic.

If a specified attack audit occurs a certain number of times in a given time period, the firewall can alert an administrator, blackhole all traffic from the IP address originating the attack, or both. Being aware of attempted attacks is an important part of maintaining your network security.

Network defenses

Sidewinder is preconfigured to block an extensive list of suspicious traffic at the data link, network, and transport layers.

Packets that do not adhere to their protocol standards are always dropped, as are packets that match known attack configurations.

Encrypted content inspection

Conventional firewalls allow encrypted connections to pass through without inspection. Sidewinder can decrypt, inspect, and re-encrypt encrypted connections for both inbound and outbound traffic.

- **SSL** — By decrypting SSL connections, the firewall can inspect their contents and enforce access control on SSL-encapsulated applications. For example, you can do the following:
 - Allow only HTTPS while denying other SSL content
 - Enable virus scanning and other HTTP Application Defense enforcements on HTTPS connections
 - Inspect inbound HTTPS connections before they reach internal web servers
- **SSH** — Use to control port forwarding, SFTP operations, and the encryption algorithm.

Global Threat Intelligence

Global Threat Intelligence spans the entire Internet, effectively using millions of sensors to gather real-time intelligence from host IP addresses, Internet domains, specific URLs, executable files, images, and email messages.

Global Threat Intelligence seeks new and emerging threats, including malware outbreaks, zero-day exploits, and malicious zombie senders generating spam and web attacks.

Web reputation

Global Threat Intelligence is a global reputation service that assigns a reputation score to an IP address or executable file based on the behavior attributes of the traffic it generates. A reputation score is like a credit score that indicates the trustworthiness.

With Global Threat Intelligence, the Sidewinder is able to infer the likelihood of malicious intent from network traffic, protecting your users from unwanted risk.

Global Threat Intelligence uses servers around the world to gather and analyze billions of packets dynamically to determine reputation scores. For each IP address or executable file on the Internet, Global Threat Intelligence calculates a reputation value based on attributes such as sending behavior, blacklist and whitelist information, and spam trap information.

You can enable Global Threat Intelligence on access control rules, allowing rules to selectively match the Global Threat Intelligence web reputation scores of your choice.

Geo-Location

Geo-Location identifies the country of origin of an IP address. Using a Geo-Location network object in an access control rule, you can allow or deny connections based on where they came from or where they are going.

Virus protection

You can create access control rules that scan HTTP traffic, FTP files, and mail messages for viruses, giving you another layer of protection.

SmartFilter web filtering

SmartFilter is a web filtering solution designed to manage access to the Internet.

Using SmartFilter mitigates your organization's exposure to viruses, malware, and other security risks, while reducing legal liability, maximizing employee productivity, and preserving bandwidth for business-related activities.

You can enable SmartFilter on access control rules to filter your users' web access.

PART I

Planning and setup

Contents

- [Planning](#) on page 21
- [Installation and configuration](#) on page 41
- [Startup](#) on page 53

Planning

Contents

- [Planning your setup](#) on page 21
- [Integration Checklist](#) on page 37
- [Quick Start Wizard Response Form](#) on page 38

Plan your considerations for setting up and integrating the Sidewinder appliance into your network environment.



Note: Some of these tasks can take several weeks. Preparation greatly reduces the disruption to your production network.

Planning your setup

This section explains the various configuration options to help you determine your initial firewall configuration.

Use the decision table in each section for an overview of the main decision and actions. The text that follows each decision table explains the topic in more detail.

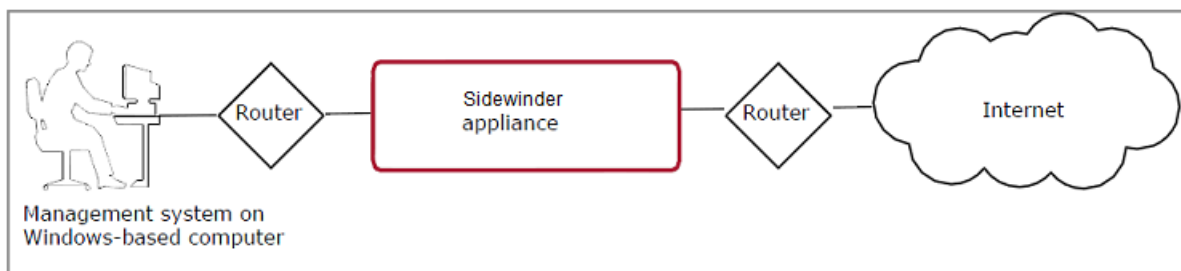
Table 1: Sample decision table

Determine your initial firewall configuration.

- 1) Print the *Quick Start Wizard Response Form*.
- 2) Review the following topics—each explains a configuration decision:
 - *Zones*
 - *Deployment options*
 - *Initial active policy*
 - *Network information*
 - *Control Center management*
- 3) Record your responses on the *Quick Start Wizard Response Form* for use when running the Quick Start Wizard.

The Sidewinder appliance contains pre-installed software. The shipment includes additional management software that you install on a Microsoft Windows-based computer, which contains:

- **Quick Start Wizard** — Assists you with the initial firewall configuration
- **Admin Console** — Used to manage your firewall

Figure 2: Basic Sidewinder appliance environment**Related concepts**[Zones](#) on page 12[Deployment options](#) on page 23[Control Center management](#) on page 36[Network information](#) on page 33**Related reference**[Quick Start Wizard Response Form](#) on page 38[Initial active policy](#) on page 32

Renaming default zones

The firewall uses a logical division of network spaces called zones. Zones divide networks from each other, and each zone connects the firewall to systems with the same security requirements.

Decide whether you want to change the default zone names.

Record your decision in Section 4 of the *Quick Start Wizard Response Form*.

A newly installed and configured firewall has two zones. Each zone is associated with a network interface and automatically assigned a default name:

- **External** — This zone handles your external network. This is often, but not always, your network connection to the Internet.
- **Internal** — This zone handles your internal network. Users on the internal network are generally trusted, so your security policy allows more traffic out through the firewall than is allowed in.

Access rules are applied to all traffic entering the firewall from any given zone. The rules enforce your security policy by controlling the direction of traffic between or within zones.

For the initial configuration, you can change the default zone names. The following naming criteria applies:

- Must contain 1–64 characters
- Must begin with a letter; the name can contain letters, digits, underscores (_), and dashes (-)



Tip: As you create your policy, there are multiple ways to configure more interfaces and zones.

Deployment options

You can deploy firewall in *Standard (routed) mode* or *Transparent (bridged) mode*.

Decide on an interface mode for the initial configuration.

- 1) Determine whether you want to use *Standard (routed) mode* or *Transparent (bridged) mode*.
 - [Conditional] If you choose standard mode, review *Network interfaces* to determine how the firewall should get its external IP address and to specify an internal IP address.
 - [Conditional] If you choose transparent mode, review *Network interfaces* to determine the IP address for the transparent interface.
- 2) Record your decisions in sections 3 and 4 of the *Quick Start Wizard Response Form*.

For traffic to pass through your firewall, it must arrive on an interface and leave on a different interface.

The internal and external network interfaces are defined during initial configuration; however, you can configure additional interfaces to suit the needs of your network infrastructure. The firewall can be used for the following (or any combination):

- Gateway between your internal network and the Internet
- Gateway between any networks with different security needs
- Transparent firewall inside a single network

The relationship between configured interfaces can be classified as:

- Standard (routed) mode
- Transparent (bridged) mode
- Hybrid mode (the firewall can be simultaneously configured with a single bridge and additional routed interfaces)
- SPAN mode (available in either Standard or Hybrid mode)

Related concepts

[Standard \(routed\) mode](#) on page 23

[Network interfaces](#) on page 29

[Hybrid mode](#) on page 30

[SPAN mode](#) on page 30

[Transparent \(bridged\) mode deployment](#) on page 25

Related reference

[Quick Start Wizard Response Form](#) on page 38

Standard (routed) mode

In this mode, a network interface connects the firewall to each network. The firewall allows traffic to pass between the networks like a router, enforcing your security policy.

The Sidewinder appliance is deployed at the intersection of multiple networks. Each firewall interface is assigned a unique IP address in the connected subnet.

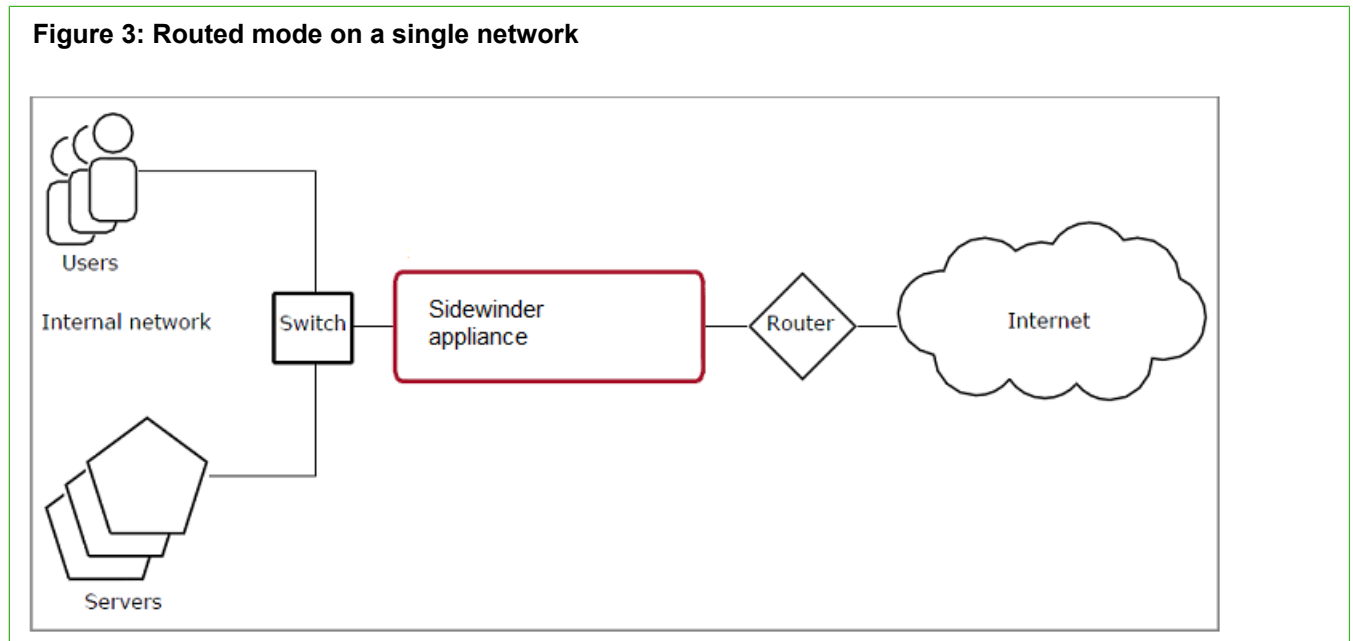
The protected networks must be unique' each network must be a different subnet. Hosts in a protected network communicate with other networks using the firewall IP address as the gateway.

Each firewall interface is assigned to a unique zone. When traffic attempts to cross from one zone to another, the configured security policy is enforced.

Protecting a single network

A firewall can protect the internal network from the Internet.

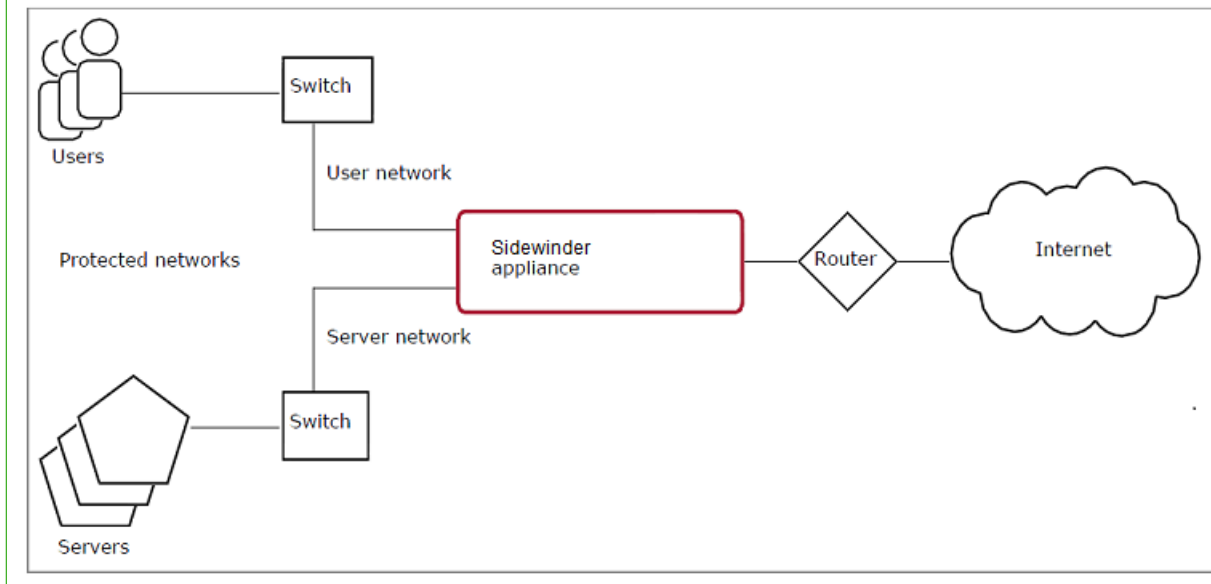
The following figure illustrates how the firewall protects the internal network. This configuration uses two network interfaces. To reach the Internet, hosts on the internal network route traffic to the firewall.



Protecting multiple networks

A firewall can protect the user and server networks from each other and the Internet.

The following figure illustrates the firewall protecting two separate networks from each other and from the Internet. This configuration uses three network interfaces. To reach the Internet or one of the other protected networks, hosts route traffic to the firewall.

Figure 4: Protecting multiple networks

Network interface IP addresses

Each network interface on the firewall must be assigned an IP address in a unique network. The networks cannot overlap.

You must assign IPv4 addresses to the network interfaces during initial configuration.



Note: The firewall supports IPv6 addresses, but IPv6 addresses cannot be assigned during initial configuration; they can be assigned after the initial configuration is complete.

- For the external IP address, consider these options:
 - **Obtain an IP address automatically** — Automatically assigns an external address using a Dynamic Host Configuration Protocol (DHCP) server.

If you select this option, an access control rule is configured to allow DNS requests to all destinations in the external zone. To improve security, you might want to modify this rule to restrict which DNS servers can be reached from your network. However, if you restrict the rule and the DNS information that is assigned via DHCP is updated, there is a possibility that legitimate DNS traffic might be denied.
 - **Specify an IP address** — If you are manually assigning an IP address, identifies a unique IP address for the external network interface.
- For the internal address, identify a unique IP address for the internal network interface.

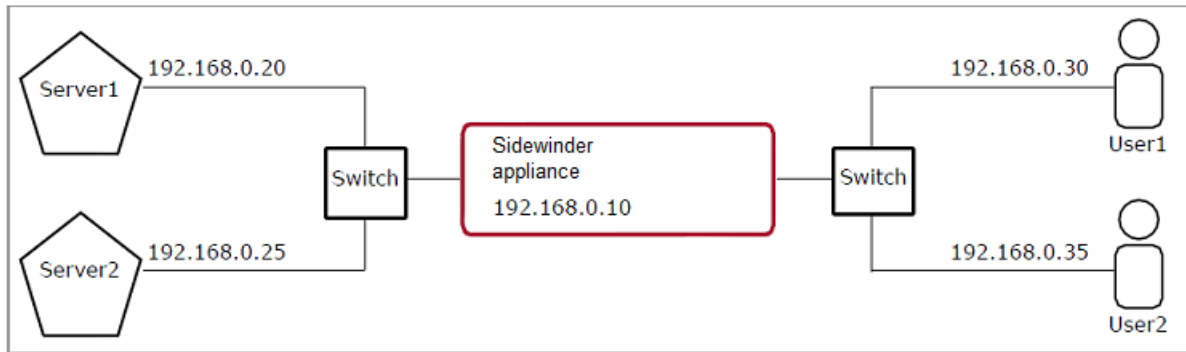


Tip: The netmask is automatically populated in the Quick Start Wizard, but you can change it if it is not correct.

Transparent (bridged) mode deployment

In transparent (bridged) mode, two or more firewall interfaces are connected inside a single network and bridged to form a transparent interface. Each interface is assigned to a unique zone. Traffic passes through the firewall like a switch, allowing you to enforce security policy inside the network without re-addressing the network.

Figure 5: Transparent mode inside a single subnet



Note: The firewall supports only one configured transparent interface (bridge) at a time.

The following table shows the default firewall interface configuration. These interfaces—or any other interfaces—can be used to configure a transparent interface.

Table 2: Standard interfaces

User defined interface name	NIC or NIC Group	Zone name
external_network	em0	external
internal_network	em1	internal

The following table shows a transparent interface configured using the default interfaces. Note that bridge0 is made up of em0 and em1.

Table 3: Transparent interface

User defined transparent interface name	NIC or NIC Group
bridged_network	bridge0 (em0, em1)

Access control rules determine if traffic is allowed to cross the transparent interface (from one zone to the other). Since hosts inside the network are not aware that the firewall is deployed, they communicate with each other as if they were directly connected by a switch.

- If two hosts reside in the same zone (the same side of the transparent interface), they communicate directly over the network, and no security policy is enforced.
- If two hosts reside in different zones (different sides of the transparent interface), they communicate through the firewall, and security policy is enforced.

Consider the deployment scenarios as follows.

Related concepts

[Transparently enforcing security policy inside a single subnet](#) on page 27

[Transparently protecting a single network](#) on page 28

Transparently enforcing security policy inside a single subnet

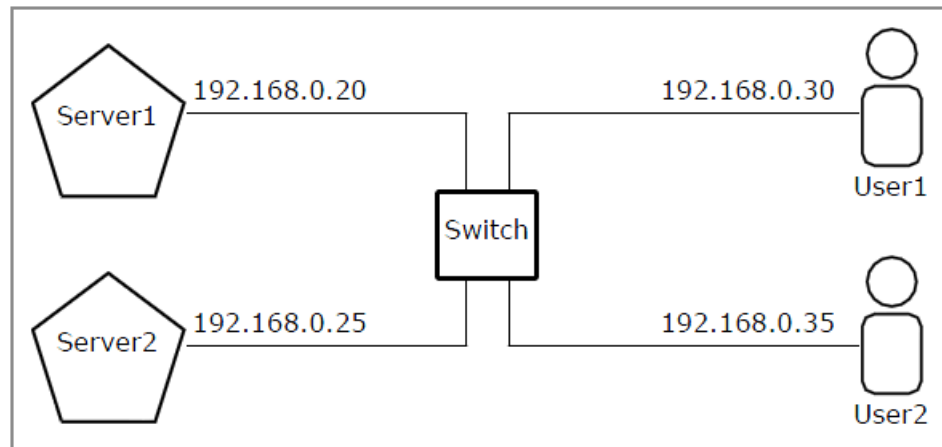
You can use the transparent mode to protect servers in a single subnet.

The following figure illustrates a single subnet (192.168.0.0/24) that contains both servers and users.

Scenario:

Assume that the network administrator is introducing a firewall to protect the servers from the users. However, the network cannot be re-addressed, and all of the servers and users must retain their current IP addresses. The Sidewinder appliance meets these requirements using the transparent mode.

Figure 6: A single subnet containing servers and users

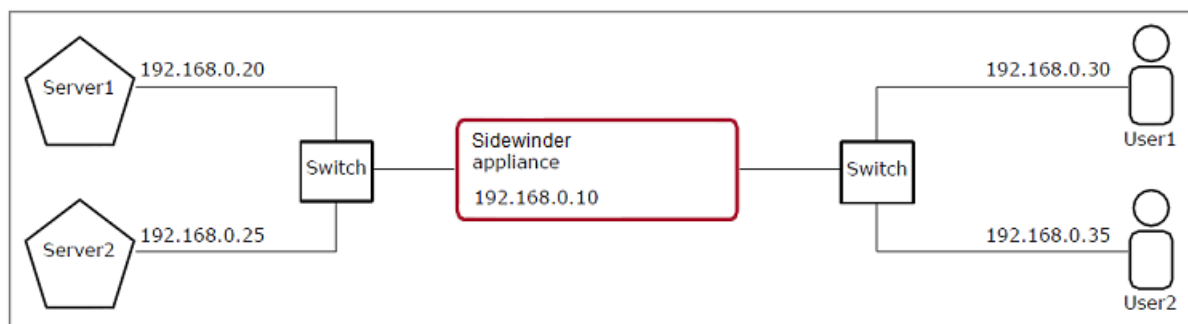


The following figure illustrates the firewall in transparent mode protecting the servers from the users. As traffic between the users and servers crosses the firewall transparent interface, it also crosses from one zone to the other. Access control rules enforce security policy on the traffic.



Note: While deploying the firewall in transparent mode does not require re-addressing the network, the firewall does require a management IP address. (In this example, 192.168.0.10 was reserved for the firewall.)

Figure 7: Transparent firewall inside a single subnet



Transparently protecting a single network

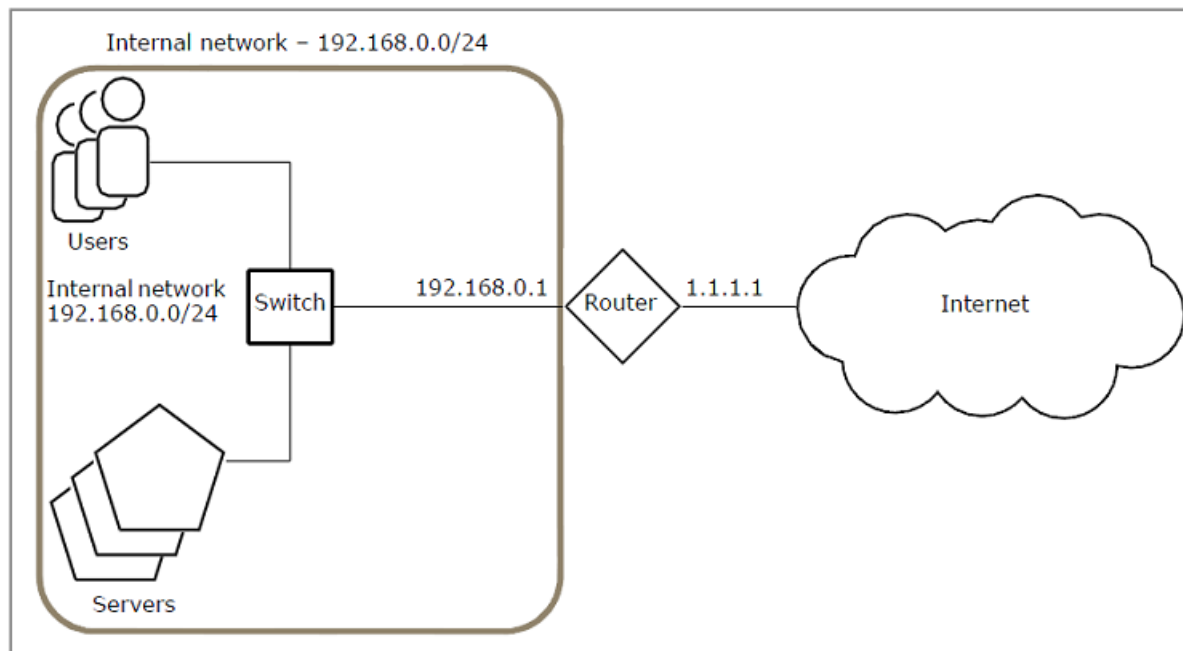
You can use the firewall in router or transparent mode to protect the internal network.

The following figure illustrates an internal network that is protected from the Internet by a router only.

Scenario:

Assume that the network administrator is introducing a firewall to protect the internal network from the Internet. However, there is a requirement that the network cannot be re-addressed, and all of the servers and users must retain their current IP addresses.

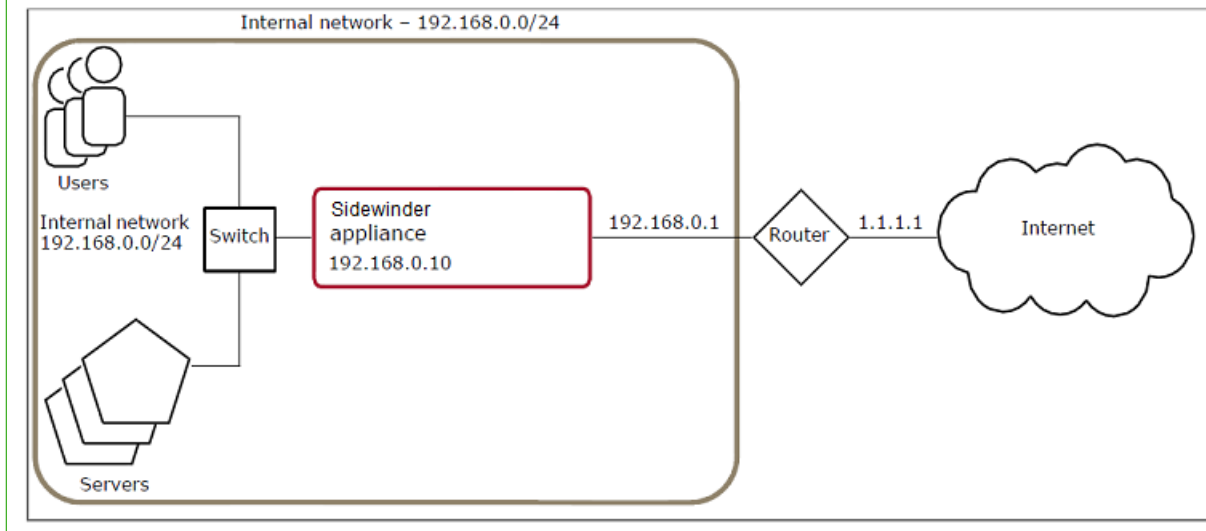
Figure 8: No firewall



There are two options for using the firewall to protect the internal network:

- Deploy the firewall in router mode, and re-address the networks around it.
- Deploy the firewall in transparent mode inside the internal network.

Using transparent mode provides an advantage—none of the networks around the firewall need to change. In addition, the hosts on the internal network will have no knowledge that the firewall has been deployed between the switch and the router as shown in the figure below.

Figure 9: Transparent firewall protecting a single network

The default route for the hosts on the internal network remains the router (192.168.0.1), which is on the other side of the firewall. As traffic bound from the internal hosts to the Internet crosses the transparent interface, it also crosses from the internal zone to the external zone. Access control rules enforce security policy on the traffic.



Note: While deploying the firewall in transparent mode does not require re-addressing the network, the firewall does require a management IP address. (In this example, 192.168.0.10 was reserved for the firewall.)

Network interfaces

Assign a management IP address for the transparent interface. This must be an IPv4 address that is unique on the bridged network.



Tip: The netmask is automatically populated in the Quick Start Wizard, but you can change it if it is incorrect.

Restrictions for transparent (bridged) mode

When you configure a transparent interface, you cannot enable or configure some features.

- Split DNS
- HA
- Sendmail
- Dynamic routing
- DHCP on the transparent interface
- DHCP Relay agent
- VPN termination in a transparent zone
- IPv6 addresses on the transparent interface



Note: A transparent interface passes traffic at layer two, similar to a bridge. Sidewinder does not run the Spanning Tree bridging protocol; therefore, we do not recommend enabling Spanning Tree on the switch that is connected to the firewall.

Hybrid mode



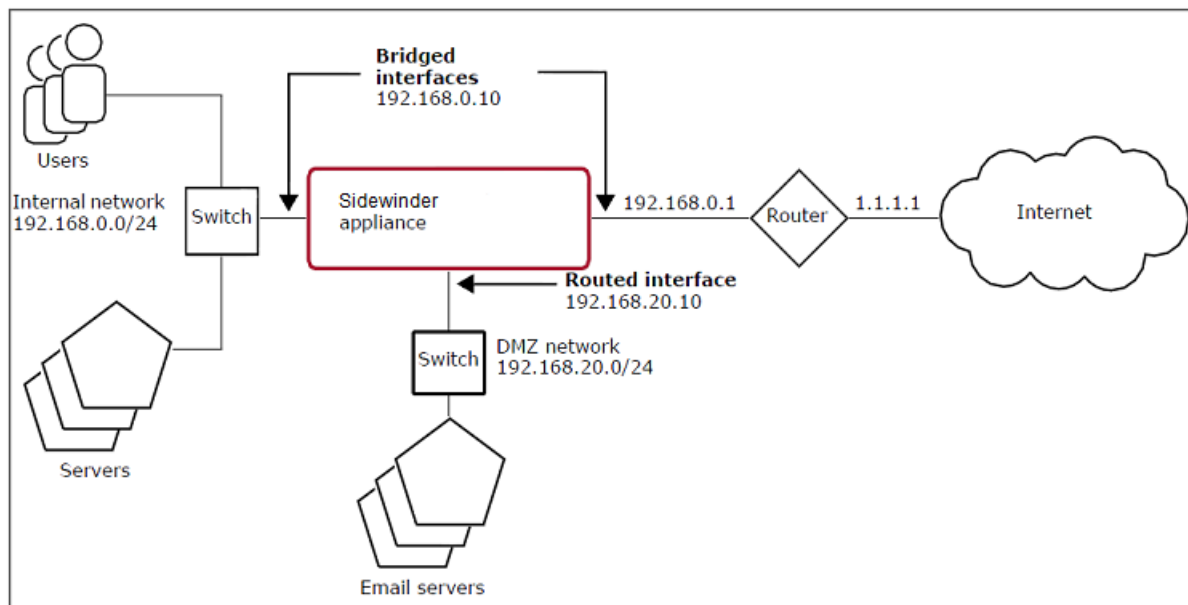
Note: This option is available after you complete your initial configuration.

The firewall can be simultaneously configured with a single bridge and additional routed interfaces. The following figure illustrates the firewall configured with a transparent interface and a routed interface. In this example, the firewall protects the internal and DMZ networks from each other and from the Internet.



Note: The firewall has two IP addresses, a transparent IP address for management (192.168.0.10, assigned to both bridged interfaces) and a routed IP address on the DMZ interface (192.168.20.10).

Figure 10: Hybrid firewall



To reach the Internet:

- Hosts in the internal network route traffic to the router's IP address (192.168.0.1) on the other side of the firewall.
- Hosts in the DMZ route traffic to the firewall's DMZ IP address (192.168.20.10).

As traffic crosses from interface to interface, it also crosses from one zone to another. Access control rules enforce security policy on the traffic.

Related concepts

[Types of interfaces](#) on page 374

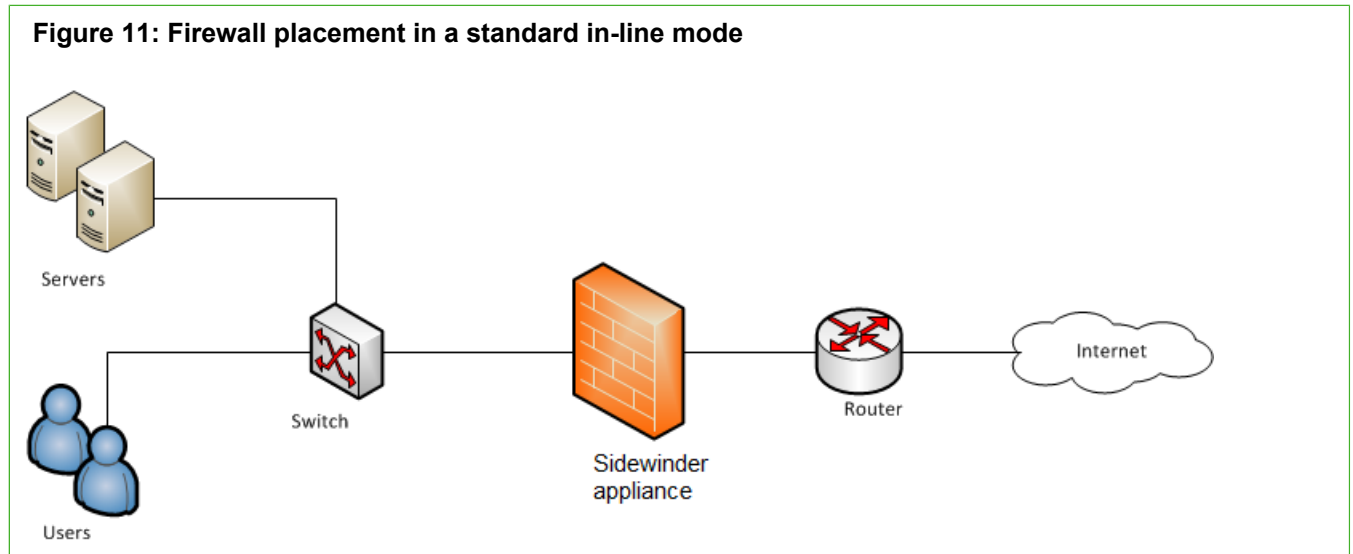
SPAN mode

In Switched Port Analyzer (SPAN) mode, the firewall passively listens on the network to analyze traffic.

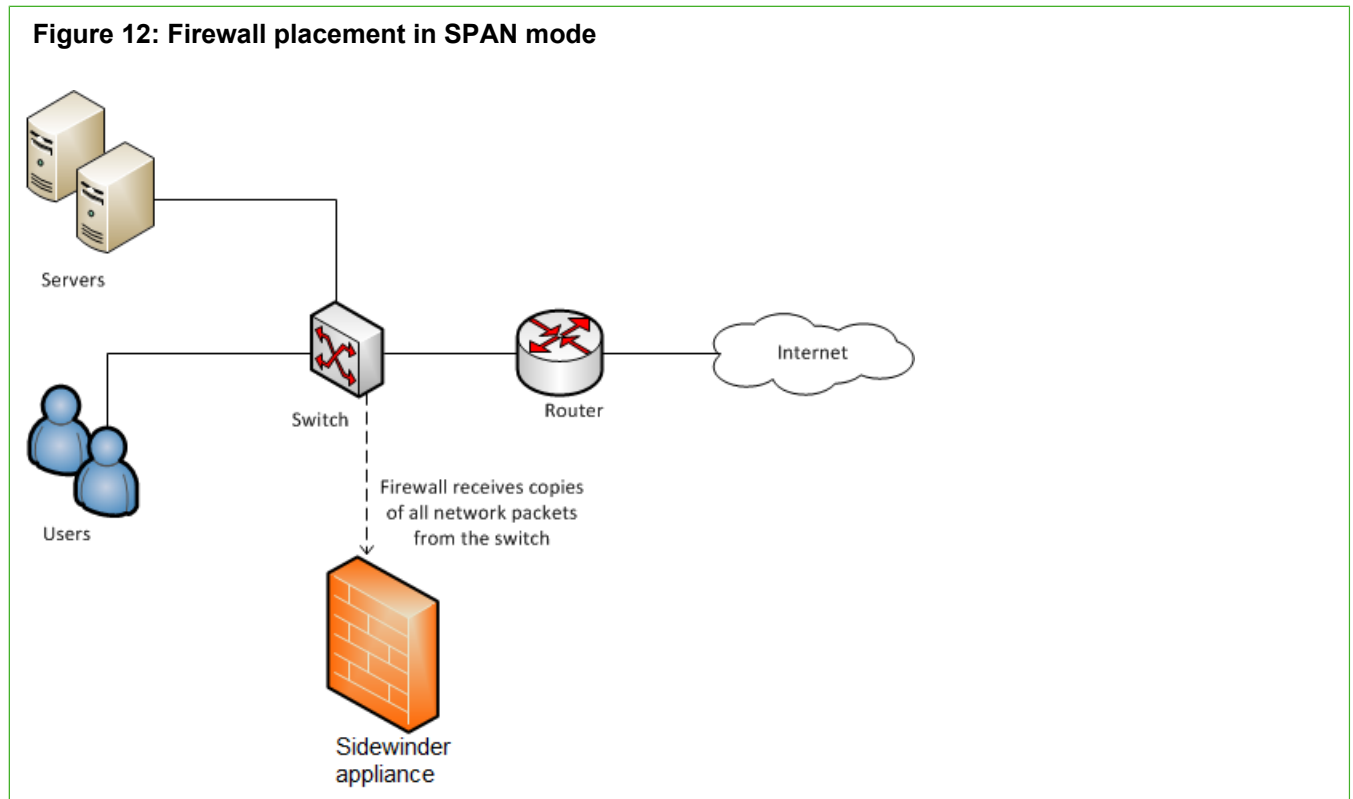
When SPAN is enabled on an interface, the firewall receives copies of all packets on the network. This allows the firewall to inspect traffic, determine the action to take, and audit accordingly without actually participating in

the connection. This mode is ideal for seeing how the firewall allows or denies traffic based on policy without impacting traffic on the network.

The figure shows the standard in-line placement of Sidewinder in a network:



This figure shows the placement of Sidewinder in a network when configured for SPAN mode:



SPAN mode can be enabled only on a standard or VLAN interface after the installation and initial configuration. Setup requires enabling SPAN mode on a per-interface basis and configuring zones and access control rules to process SPAN traffic.



Note: Sidewinder can process in-line and SPAN traffic at the same time but not on the same interface. Separate interfaces must be configured for in-line and SPAN traffic.

Related concepts

[SPAN interfaces](#) on page 376

Related tasks

[Create a SPAN interface](#) on page 385

[Create a SPAN policy](#) on page 272

Initial active policy


A new Sidewinder appliance includes a set of preconfigured rules on the **Rules** window. Some rules are enabled by default to allow firewall administration. Other rules are not enabled by default and, therefore, do not pass traffic.

Select an initial rule group.

Record your decision in section 3 of the *Quick Start Wizard Response Form*.

Consider the following default policy options for the initially configured firewall.

Table 4: Default policy options

Option	Definition
<p>Allow administrative services only</p>	<p>Enables only the Administration rule group, which contains preconfigured access control rules that are necessary for firewall administration:</p> <ul style="list-style-type: none"> • dnsp (names vary) — Allows DNS clients in all zones through to the external zone resolvers • Login Console — Allows administrators to log on directly at the firewall using an attached keyboard and monitor • Admin Console — Allows administrators to connect to the firewall using the Admin Console • Passport — Allows authentication to the Passport server and facilitates the use of single sign-on authentication • Deny All — Denies all connections from any source zone to any destination zone <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Note: Other preconfigured rules appear on the Rules window by default; however, they are not enabled and do not pass traffic.</p> </div>

Option	Definition
<p>Allow administrative and basic outbound Internet services</p>	<p>Enables the following default policy:</p> <ul style="list-style-type: none"> • Administration rule group — Contains preconfigured access control rules that are necessary for firewall administration. • Internet services rule — Allows users access to the most commonly used Internet services; the preconfigured Internet Services application group regulates access to the following applications: <ul style="list-style-type: none"> • FTP • HTTP • HTTPS • Ping • Real Media • RTSP • Telnet
<p>Allow all (transparent mode only)</p>	<p>Enables the following default policy:</p> <ul style="list-style-type: none"> • Administration rule group — Contains preconfigured access control rules that are necessary for firewall administration. • Allow all rule group — Contains three access control rules that allow all traffic to pass between the transparent (bridged) interfaces: <ul style="list-style-type: none"> • Allow All tcp and udp — Allows all TCP and UDP traffic between the bridged zones • Allow All icmp — Allows all ICMP (ping) traffic between the bridged zones • Allow All other protocol — Allows all other protocols traffic between the bridged zones

Related reference

[Quick Start Wizard Response Form](#) on page 38

Network information

Identify the network information for the firewall.
<ol style="list-style-type: none"> 1) Determine the following: <ul style="list-style-type: none"> • DNS resolver IP addresses • Default route • Internal mail host • Host name for the firewall 2) Record your decisions in sections 4 and 5 of the <i>Quick Start Wizard Response Form</i>.

Transparent DNS offers a simplified DNS configuration. When you configure transparent DNS for the firewall, DNS traffic passes transparently through the firewall. The firewall uses rules to pass all DNS traffic to the appropriate zone.



Note: In transparent DNS mode, the firewall does not host any DNS servers. Instead, DNS rules allow DNS traffic to pass through the firewall to remote name servers.

Related reference

[Quick Start Wizard Response Form](#) on page 38

DNS resolver IP addresses

Select the primary and secondary DNS resolver IP addresses.

- **Primary** — IP address of the main DNS resolver that will handle the firewall DNS requests
- **Secondary** — IP address of a backup DNS resolver that the firewall queries if the primary IP address does not respond



Note: This option is not available for firewalls using DHCP.



Tip: You can use a different primary DNS resolver in the other zone (one in the external zone, another in the internal zone). You can also use an alternate server in the same zone.

Default route

Traffic between computers on different networks or subnets requires routing. Each computer must be configured with where to send traffic it cannot deliver directly. Traffic generally goes to a router that allows access to distant subnets.

Determine the default route. A default route is a route of last resort and defined as the IP address where packets are forwarded that have no explicit route. A default route is usually the IP address of a router that forwards packets to your Internet Service Provider (ISP).

Internal mail host

Designate an internal mail host to forward all mail addressed to users on your internal network.

Related concepts

[Types of DNS modes](#) on page 459

Additional administration route

You need to add a static or remote administration route when running the Quick Start Wizard.

Define a static route for reaching your remote management console.

Record your decision in Section 6 of the *Quick Start Wizard Response Form*.

[Conditional] The computer running the Admin Console and your firewall must be able to connect to each other. If they are not on the same network and cannot connect through the default route, you must define a static route. If no static route exists, you must add a static route, or *remote administration route*, when you run the Quick Start Wizard.

This route can be to a specific host or to an entire subnet. Other routes can be added after the firewall is operational.

If you need a route to begin managing your firewall, enter the Admin Console computer IP address or subnet; then enter the IP address of the gateway (router) to reach that IP address/subnet.



Note: You will not have the option of configuring another administration route during the Quick Start Wizard.

Related reference

[Quick Start Wizard Response Form](#) on page 38

Administrator information

You need to add details for an administrator user account when running a Quick Start Wizard.

Determine the user name and password for connecting to the firewall.

Record your decision in Section 7 of the *Quick Start Wizard Response Form*.

Related reference

[Quick Start Wizard Response Form](#) on page 38

Administrator user name and password

You need to create a user name and password that you will use to connect to the firewall.

- The user name must be between 1–16 alphanumeric characters.
- We recommend using strong passwords:
 - Minimum of eight characters.
 - Mix of uppercase, lowercase, numeric, and special characters.

Use alternate administrator email address

By default, status updates and alerts are emailed to the administrator's mailbox on the firewall. You can enter an email address that is on or off the firewall to receive these messages instead.

Control Center management

You can manage a firewall using Control Center.

Do you want to use the Forcepoint Sidewinder Control Center rapid deployment option?

Record your decision in section 2 of the *Quick Start Wizard Response Form*.

[Conditional] If you are using a Control Center appliance to manage the firewall, you can use the Quick Start Wizard to automatically register the firewall.



Note: Do not use rapid deployment if you intend to use the firewall in a managed HA cluster.

Only firewalls at version 7.0.0.04 and higher can be managed by a Control Center appliance. Management support is also dependent on the Control Center version. Refer to the Control Center [Release Notes](#) for version compatibility information.



Note: When you register with Control Center, the firewall automatically creates an administrator account named *ccfwadmin*. If you already have an administrator account with that name, it will be overwritten.

To use rapid deployment, you will need:

- Fully qualified domain name (FQDN) of the Control Center Management Server
- IP address of the Control Center Management Server



Note: If you are using a High Availability Management Server configuration, use the FQDN and IP address of the active Management Server.

- Password for use in enrolling the firewall with the Control Center server; the password must be between 8-256 characters

[Optional] To quickly populate the Control Center server Sign Up window, save the password information in a text file, then import it into the Control Center server when you initiate rapid deployment.

- **Default password** — If you are using a default password, list the host names and IP address of all security devices using that password. Separate the columns with spaces, and press **Enter** to start a new row.
- **Unique password** — If you are using a unique password for each security device, list only one security device per file. Separate the columns with spaces.



Tip: You can initiate rapid deployment using the Control Center **Sign Up Firewalls** window.

Related reference

[Quick Start Wizard Response Form](#) on page 38

Integration Checklist

Print this checklist to help you prepare and schedule your firewall integration tasks.

Network information

- [Conditional] If you are new to the Sidewinder appliance, we recommend that you review network perimeter security concepts and basic issues for integrating a firewall into your existing network.
- Organize your network information. Prepare a diagram that indicates where you will place firewalls in your existing network. Include the following:
 - Routers, mail servers, web servers, FTP servers, and DNS servers
 - Internal or partner networks and their routes

Internet connection and registration considerations

- Verify that your site has an Internet connection. If you do not already have a connection, obtaining one might take several weeks. Contact your ISP for assistance with this task.
- Verify that your site IP address and domain name are registered with an Internet registration association. Contact your ISP for assistance with this task.
- [Conditional] If you plan to use the firewall-hosted DNS or secure split SMTP servers, you can use the Admin Console to configure them after the initial configuration is complete. Before you configure them, make sure you address the following issues:
 - [Conditional] If your company has an existing Internet presence, notify your ISP of the date your network traffic will start flowing through the firewall. The ISP must change your mail exchanger (MX) and name server records to point to the firewall's external IP address.
 - Notify ICANN (or equivalent domain registrar) that your firewall will be an authoritative name server for your domain.

Support staff and materials considerations

- Schedule experts for your existing network components to be onsite or available during installation.
- Schedule experts for Internet services and applications that will interact with the firewall to be onsite or available during installation.
- Locate any documentation that can be useful if problems occur.

Network services downtime considerations

- Develop a test plan to verify that all key services are functioning as desired.
- Schedule an appropriate amount of time for the installation. Include time for:
 - Preparation
 - Physical firewall installation
 - Testing critical features and services




Note: An experienced firewall installer requires approximately eight hours to install, configure, and test a basic installation. Adjust this time accordingly based on your experience and the complexity of your security policy and test plan.

- Inform your users and help desk when the network will be unavailable. Include information about any new access controls that will affect their use of the network.

Quick Start Wizard Response Form

Print this form, and record your Quick Start Wizard responses. You will use these responses during initial configuration.

1. License Information

License Information	
Serial Number  <div style="background-color: #f0f0f0; padding: 5px; margin-left: 20px;"> Tip: You can find your serial number on the Activation Certificate and attached to the top of the appliance. </div>	
Contact Information	
First Name	
Last Name	
Phone Number	
Email	
Purchased From	
Company Information	
Name	
Street	
City	
State/Province	
Postal (Zip) Code	
Country	

2. Control Center Management

Control Center Management	
Primary Server host name	
Primary Server IP address	
Sign Up password	

3. Initial Policy

Initial Policy	
<ul style="list-style-type: none"> • Interface mode <ul style="list-style-type: none"> • Standard • Transparent • Rule group <ul style="list-style-type: none"> • Allow administrative services only • Allow administrative and basic outbound Internet services • Allow all (transparent mode only) <ul style="list-style-type: none"> • Allow All tcp and udp • Allow All icmp • Allow All other protocol 	

4. Host name and Network Location

Host name and Network Location	
Standard (routed) mode	
Host name	
Network interfaces <ul style="list-style-type: none"> • external <ul style="list-style-type: none"> • Obtain an IP address automatically (DHCP) • Specify an IP address <ul style="list-style-type: none"> • IP address • Netmask • internal <ul style="list-style-type: none"> • IP address • Netmask 	
Zones <ul style="list-style-type: none"> • External (Internet) zone • Internal zone 	
Transparent (bridged) mode	
Host name	
Transparent interface setup <ul style="list-style-type: none"> • IP address • Netmask 	

Host name and Network Location	
Zones <ul style="list-style-type: none"> External (Internet) zone Internal zone 	

5. Network information

Network information	
DNS Resolver IP Addresses Primary Secondary (optional)	
Default route	
Internal Mail Host	

6. Additional Administration Route

Additional Administration Route	
Host	
IP Address Gateway	
Net	
IP Address Netmask Gateway	

7. Administrator Information

Administrator Information	
Administrator user name	
Password	
Use alternate administrator email address	

Installation and configuration

Contents

- [Requirements](#) on page 41
- [Install the Management Tools](#) on page 42
- [Configure Sidewinder](#) on page 43
- [Configure using other methods](#) on page 46


Install Sidewinder and complete the initial configuration. You can also consider alternate configuration methods.

Requirements

Before you begin, make sure that your management computer meets the minimum requirements and you have the necessary hardware.

To install the Management Tools, you must provide a management computer that meets the minimum requirements listed in the following table.



Table 5: Management computer minimum requirements

Component	Minimum requirements
Operating system	<p>One of the following Microsoft operating systems:</p> <ul style="list-style-type: none"> • Windows Server 2008 • Windows 7 • Windows 8 • Windows 10 <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Note: Windows 8 and Windows 10 are supported in traditional desktop mode. Tablet mode is not supported. Touchscreen is not supported.</p> </div> <p>Compatible legacy Microsoft operating systems:</p> <ul style="list-style-type: none"> • Windows XP Professional • Windows Vista
Web browser	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer, version 7 or later • Mozilla Firefox, version 3.0 or later

Component	Minimum requirements
Hardware	At minimum: <ul style="list-style-type: none"> • 2 GHz x86-compatible processor • 2 GB of system memory • 300 MB of available disk space • CD-ROM drive • 1024 x 768 display • Network card (to connect to your firewall) • USB port

To configure your firewall, you must provide the items listed in the following table.

Table 6: Required hardware

Item	Purpose
Monitor	Provide a display for the appliance.
Keyboard	Provide input for the appliance.
Network cables	Connect the appliance to the appropriate networks.
USB drive or serial cable	Transfer the initial configuration file from the management computer to the appliance. <ul style="list-style-type: none"> • USB drive — Must be formatted with the FAT, FAT16, or FAT32 file system <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;">  CAUTION: If an installation USB drive is included in your shipment, do not save a configuration file to it. </div> <ul style="list-style-type: none"> • Serial cable <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;">  Note: Use a serial console cable: 6ft, RJ-45 to DB-9 female, part number 403-1132-00. </div>

Install the Management Tools

Install the Management Tools on a Windows-based computer.

The Sidewinder Management Tools include:

- **Quick Start Wizard** — Creates the initial configuration
- **Admin Console** — Used to manage the firewall



Note: Sidewinder management tools are version-specific. Make sure you install the current version of the Admin Console—you cannot connect to a version 8.x firewall using an older version of the Admin Console. You can have multiple management tools that co-exist on the same Windows-based computer.

Steps

- 1) Insert the media into the appropriate drive.
 - **Sidewinder with CD-ROM drive** — If your Sidewinder appliance has a CD-ROM drive, install using the Management Tools CD .
 - **Sidewinder without CD-ROM drive** — If your Sidewinder appliance does not have a CD-ROM drive, install using the installation USB drive.

The Welcome window appears.



Note: If the InstallShield program does not start automatically, use Windows Explorer to view the media contents, then go to `\\Install\\Setup.exe`.

- 2) Follow the on-screen instructions to complete the setup program. We recommend using the default settings.



Tip: You should also install an SSH client on your computer. An SSH client can be used to provide secure command line access to the firewall.

Configure Sidewinder

The configuration includes several main activities.

We recommend that you follow this process to configure Sidewinder.

Steps

- 1) Set up your firewall appliance and cables.
- 2) Use the Quick Start Wizard to create a configuration file and save it to a USB drive.
The file should be saved as `qsw_datafile`.
- 3) Plug the USB drive into the firewall, and turn on the appliance. The firewall automatically loads the configuration information from the USB drive.



Note: Alternative configuration methods are available that require connecting through the Admin Console or directly to the appliance.

Related tasks

[Configure using other methods](#) on page 46

Set up the hardware

Use this procedure to set up your hardware.

You will need these items:

- Quick Start Wizard responses you collected on the *Quick Start Wizard Response Form*

- Management Tools installed on a Windows-based computer
- USB drive



Note: Do not use the installation USB drive.

Set up the Sidewinder appliance and cables.

Steps

- 1) Use a diagram of your network to determine the proper Sidewinder placement. The firewall must be able to reach the appropriate routers, subnets, and servers (such as mail servers and name servers).
- 2) Attach the power cord to the firewall, and plug it into an electrical outlet.
 - Do not turn on the firewall.
 - If your firewall has redundant power supplies, attach and plug in both power cords. If only one power supply is connected, the amber indicator blinks, indicating an error.
- 3) Connect two network cables for access to:
 - External network
 - Internal network



Note: Pay close attention to the cable you connect to each network interface. See the *Port Identification Guide* included in your shipment for cabling information specific to your model. If you cannot find your model, visit <https://support.forcepoint.com> to obtain the latest *Port Identification Guide*.

- 4) [Optional] Connect a display to the firewall using one of these methods:
 - Terminal or terminal emulator connected to the serial port (use a serial console cable, 6ft, RJ-45 to DB-9 female, part number 403-1132-00)
 - Monitor and keyboard connected to the VGA port

Related concepts

[Planning your setup](#) on page 21

Related tasks

[Install the Management Tools](#) on page 42

Related reference

[Quick Start Wizard Response Form](#) on page 38

[Integration Checklist](#) on page 37

Run the Quick Start Wizard

Run the Quick Start Wizard on your Windows-based computer.

Steps

- 1) Insert a USB drive into your Windows-based computer.
- 2) From the Windows desktop, select **Start > All Programs > Forcepoint > Sidewinder v8 Admin Console > Quick Start Wizard**.
- 3) Read and accept the License Agreement.
- 4) Follow the Quick Start Wizard instructions.
 - Use the responses you collected on the *Quick Start Wizard Response Form*.
 - Answer all questions as appropriate for your site.



Tip: For option descriptions, click **Help**.

- 5) Save configuration file to the USB drive.
The file should be saved as `qsw_datafile`.

Related concepts

[Planning your setup](#) on page 21

Related reference

[Quick Start Wizard Response Form](#) on page 38

[Integration Checklist](#) on page 37

Apply the configuration

Load the configuration and apply it to Sidewinder.

Steps

- 1) Insert the USB drive containing the Quick Start Wizard configuration file into a USB port on your firewall.
- 2) Turn on the Sidewinder appliance.
 - The firewall automatically loads the configuration information. If you have a terminal or monitor connected to the firewall, messages appear during the configuration.
 - When configuration is complete, the firewall connects to the activation server to automatically activate the license. If you receive a message, "Unable to get license from server," you must activate the license manually after you log on to the firewall. When the configuration and licensing process completes, a login prompt appears.
- 3) Remove the USB drive from the USB port.

Configure using other methods

The following procedures explain alternative configuration methods. These methods require connecting through the management computer or directly to the appliance.



Note: We recommend that you use the procedure in *Configure Sidewinder*.

Related concepts

[How to use the Admin Console default settings](#) on page 46

[How to use a locally attached terminal](#) on page 49

[How to use a locally attached management system](#) on page 51

Related tasks

[Configure Sidewinder](#) on page 43

How to use the Admin Console default settings

With this method, you can start up the appliance, then log on to the Admin Console using the factory default configuration settings.

The appliance searches for a configuration file from the command line, PXE boot, USB drive, or a serial port connected to Sidewinder. If the appliance does not find one and there is no response at the command line, the appliance loads the default settings.

Field	Default setting
Internal IP address	192.168.1.250 Note: The Admin Console access control rule that is automatically created is set to the internal zone.
External IP address	192.168.2.250
Netmask	255.255.255.0 (both interfaces)
Default gateway	192.168.1.1
Username	admin
Password	admin You will be required to change the password upon login. Tip: Passwords must be at least eight alphanumeric characters long. We recommend using a mix of uppercase, lowercase, numeric, and special characters.

Field	Default setting
Host Name	<MACAddress>_fwlocal.com Where <MACAddress> is the MAC address of the first interface.
DNS	192.168.1.254
Interface type	[S] (standard)
Administrative privileges	[A] (administrator authority)
Managed by Control Center	[N] (not Control Center managed)
Serial number	00-00000000
Other fields	<p>Below is a list of the fields that have an initial value of XXXXX</p> <ul style="list-style-type: none"> • First Name • Last Name • Phone • Email • Purchased From • Company • Address • City • State • Country • Postal code • License comments

Prepare the firewall

Set up your firewall and cables.

Steps

- 1) Use a diagram of your network to determine the proper placement of your firewall. Your firewall must be able to reach the appropriate routers, subnets, and servers (such as mail servers and name servers).
- 2) Attach the power cord to the system, and plug it into an electrical outlet.



Tip: If your appliance has redundant power supplies, attach and plug in both power cords. If only one power supply is connected, the amber indicator blinks, indicating an error.

3) Connect two network cables for access to:

- External network
- Internal network

The Sidewinder appliance network port 1 must be connected to a network. If it is not connected, the default configuration will not be applied.



Note: Pay close attention to the cable you connect to each network interface. See the *Port Identification Guide* included in your shipment for cabling information specific to your model. If you cannot find your model, visit <https://support.forcepoint.com> to obtain the latest *Port Identification Guide*.

Result



CAUTION: Do *not* turn on your firewall.

Connect with the Admin Console

Sidewinder includes default configuration settings that allow you to complete the configuration from the Admin Console.

Before you begin

Make sure the Sidewinder appliance network port 1 is connected to a network. If it is not connected, the default configuration will not be applied.

Steps

1) Turn on the appliance and wait for the configuration to load from the default factory settings.



Note: When the appliance does not find a configuration file and there is no response within 60 seconds at the command line, the appliance loads the default settings.

2) If you want to designate the IP address and netmask of the internal interface, you must access the appliance through the console.

- a) Press **Enter** when the appliance searches for the configuration.
- b) Press **M** for minimal configuration and follow the prompts.

3) Connect your management computer to the same network you used for network port 1.

4) Start the Admin Console by selecting **Start > All Programs > Forcepoint > Sidewinder v8 Admin Console > Admin Console**.

5) Connect to the firewall internal IP address using the default settings.

- 6) Follow the prompts to change your password.



Tip: Passwords must be at least eight alphanumeric characters long. We recommend using a mix of uppercase, lowercase, numeric, and special characters.

- 7) Review the license agreement and accept.

Result

You are now logged on to the firewall and can update the configuration as needed.

How to use a locally attached terminal

With this method, you attach a console to Sidewinder and run a text-mode Quick Start Program to create the initial configuration.

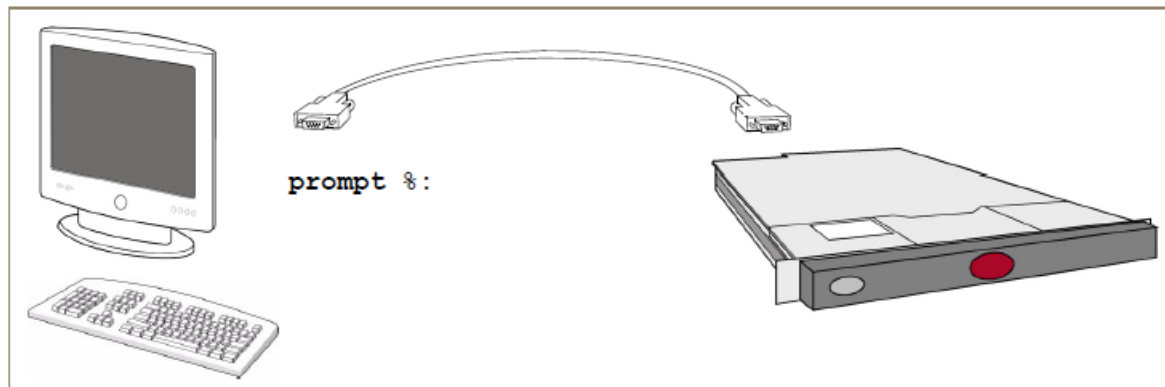
You can use either of the following:

- Terminal or terminal emulator connected to the serial port (use a serial console cable, 6ft, RJ-45 to DB-9 female, part number 403-1132-00)
- Monitor and keyboard connected to the VGA port



Note: Available ports vary by model.

Figure 13: Connect directly with the text-mode Quick Start Program



Prepare the firewall

Set up your firewall and cables.

Steps

- 1) Use a diagram of your network to determine the proper placement of your firewall. Your firewall must be able to reach the appropriate routers, subnets, and servers (such as mail servers and name servers).

- 2) Attach the power cord to the system, and plug it into an electrical outlet.



Tip: If your appliance has redundant power supplies, attach and plug in both power cords. If only one power supply is connected, the amber indicator blinks, indicating an error.

- 3) Connect two network cables for access to:

- External network
- Internal network



Note: Pay close attention to the cable you connect to each network interface. See the *Port Identification Guide* included in your shipment for cabling information specific to your model. If you cannot find your model, visit <https://support.forcepoint.com> to obtain the latest *Port Identification Guide*.

- 4) Turn on your firewall.
- 5) Connect a keyboard and monitor to the VGA port, or connect a terminal or terminal emulator to the serial port.

Configure the serial connection

If you are using a terminal, select a terminal emulator software program, and set the parameters listed in the table.

Table 7: Serial connection parameters

Port setting	Value
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

Run the Quick Start Program

After the firewall starts up and the systems connect, a “Welcome to the Quick Start Program” message appears on the terminal.

Steps

- 1) Follow the on-screen prompts to enter the configuration information.
 - Use the responses you collected on the *Quick Start Wizard Response Form*.
 - Answer all questions as appropriate for your site.

- 2) Review and accept the configuration responses. Messages appear while the configuration is applied.
 - When configuration is complete, the firewall connects to the activation server to automatically activate the license.



Note: If you receive a message, “Unable to get license from server,” you must activate the license manually after you log on to the firewall.

- When the configuration and licensing process completes, a login prompt appears.

Related reference

[Quick Start Wizard Response Form](#) on page 38

[Integration Checklist](#) on page 37

How to use a locally attached management system

With this method, you connect the Windows-based computer with Management Tools directly to the firewall using a serial cable, then run the Quick Start Wizard and apply the configuration to the firewall using the serial cable.

Prepare the management system

Initiate preparing the management system with these items.

- Quick Start Wizard responses you collected on the *Quick Start Wizard Response Form*
- Management Tools installed on a Windows-based computer

Related reference

[Quick Start Wizard Response Form](#) on page 38

Prepare the firewall

Set up your firewall and cables.

Steps

- 1) Use a diagram of your network to determine the proper placement of your firewall. Your firewall must be able to reach the appropriate routers, subnets, and servers (such as mail servers and name servers).
- 2) Attach the power cord to the system, and plug it into an electrical outlet.



Tip: If your appliance has redundant power supplies, attach and plug in both power cords. If only one power supply is connected, the amber indicator blinks, indicating an error.

3) Connect two network cables for access to:

- External network
- Internal network



Note: Pay close attention to the cable you connect to each network interface. See the *Port Identification Guide* included in your shipment for cabling information specific to your model. If you cannot find your model, visit <https://support.forcepoint.com> to obtain the latest *Port Identification Guide*.

4) Using a serial cable, connect one end of the cable to the firewall and the other end to a Windows-based computer containing the Management Tools.



Note: Use a serial console cable, 6ft, RJ-45 to DB-9 female, part number 403-1132-00.

5) Turn on your firewall.

Run the Quick Start Wizard

Run the Quick Start Wizard from the Windows desktop.

Steps

- 1) Select **Start > All Programs > Forcepoint > Sidewinder v8 Admin Console > Quick Start Wizard**.
- 2) Read and accept the License Agreement.
- 3) Follow the Quick Start Wizard instructions.
 - Use the responses you collected on the *Quick Start Wizard Response Form*.
 - Answer all questions as appropriate for your site.



Tip: For option descriptions, click **Help**.

- 4) From the Quick Start Summary window, apply the configuration to the firewall.

Related concepts

[Planning your setup](#) on page 21

Related reference

[Quick Start Wizard Response Form](#) on page 38

[Integration Checklist](#) on page 37

Contents

- [What the Admin Console does](#) on page 53
- [Activating the license](#) on page 56
- [Complete post-setup tasks](#) on page 61

To start using the firewall, you need to use the Admin Console to connect to the firewall, activate the license, and complete post-setup tasks.

Related concepts

[Admin Console access management](#) on page 565

What the Admin Console does

Use the Admin Console to connect to and manage one or more firewalls.

The *Admin Console* is the primary user interface for the firewall. The firewall policy must allow Admin Console access for the zone the Admin Console computer resides in. By default, access is enabled on the internal zone.



Note: Make sure you use the Admin Console version that you installed.

Related tasks

[Install the Management Tools](#) on page 42

Navigating through the Admin Console

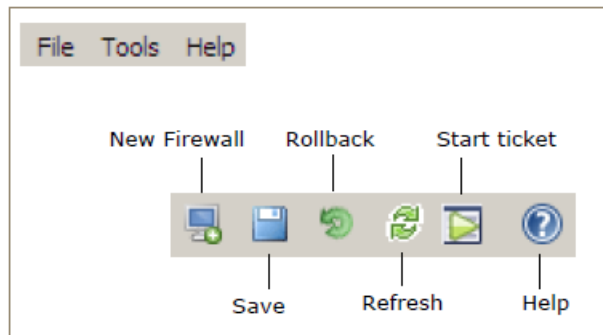
The Admin Console contains three main sections.

- Toolbar
- Left pane
- Right pane

Toolbar

The toolbar contains menus and buttons for completing a variety of actions.

Figure 14: Admin Console menu and toolbar



Tip: For option descriptions, click **Help**.

Add a firewall and connect

Using the information on the *Quick Start Wizard Response Form*, add a firewall and connect to it.

Steps

- 1) From a Windows desktop on your internal network, select **Start > All Programs > Forcepoint > Sidewinder v8 Admin Console > Admin Console**.
- 2) Add a firewall to the Admin Console.
 - a) From the toolbar, click **New Firewall**. The **Add Firewall window** appears.
 - b) Complete the information.
 - c) Click **Add**.

The firewall appears in the Admin Console tree.



Tip: If a message appears stating "Failed to connect to SSL server," the firewall might not have finished restarting. Wait a few minutes, then try connecting again.

- 3) To connect, select the firewall in the left pane, then click **Connect**.
- 4) [Initial connection only] A pop-up window appears with the firewall certificate that will be used for with all subsequent administrative connections.
 - **Accept** — To accept the certificate, click **Yes**. The Login window appears.
 - **Verify** — To verify the certificate before accepting it, you must obtain the certificate fingerprint before you log on to the Admin Console.



Note: If you have not configured remote access, you will need to attach a monitor and keyboard directly to your firewall.

- Using command line, log on to the firewall.
- Type `srrole` to change to the Admn domain.
- Enter the command: `cf cert view fw name=Default_SSL_Cert`. The contents of the certificate appear.
- Locate the certificate fingerprint at the bottom of the certificate directly beneath the END CERTIFICATE identifier. Use this fingerprint to verify the fingerprint that appears when you initially connect to the firewall via the Admin Console.

- 5) Log on to the firewall.
 - a) From the Admin Console tree, select the firewall and click **Connect**. The **Login** window appears.
 - b) Type the administrator's user name, then click **OK**. The **Password Authentication** window appears.
 - c) Type the password, then click **Enter**. The **Feature Notification** window appears listing the features that are licensed on your firewall.



Tip: If you do not want this window to appear again for any firewall, select the **Don't show this again** checkbox.

- 6) Click **Close**. The main Admin Console window appears, and you are connected to the Sidewinder appliance.

Related concepts

[Activating the license](#) on page 56

[Planning your setup](#) on page 21

[Startup](#) on page 687

Disconnect from a firewall

End an Admin Console session for a firewall.

Steps

- 1) In the left pane, select the firewall.
- 2) In the right pane, click **Disconnect**.
The firewall disconnects from the Admin Console.



Note: Disconnecting does not shut down the firewall.



Tip: For option descriptions, click **Help**.

Activating the license

After you log on, the firewall automatically attempts to activate the license.

- If the license activates, a window appears listing the features currently licensed for that firewall.
- If a message appears, "Unable to get license from server," you must activate the license manually. Until the license is activated, the firewall operates using a trial license that is valid for 30 days. A trial license includes:
 - Firewall
 - Support
 - Global Threat Intelligence
 - IPS
 - Application
 - Geo Location
 - Anti-Virus

Related tasks

[Configure the license tabs](#) on page 59

[Verify a license](#) on page 56

[Manually activate a license](#) on page 57

Verify a license

Verify a firewall license and its associated features.

Steps

1) From the Admin Console, select **Maintenance > License**.

2) Click the **Firewall** tab.



Tip: For option descriptions, click **Help**.

3) Examine the **Activation Key** field to determine if the firewall license is activated.

- If the field is populated with a key, the firewall license is activated.
- If the field is blank, the firewall license did not automatically activate. Manually activate the firewall license to prevent it from expiring after the trial period ends.

Related concepts

[Licensing](#) on page 688

Manually activate a license

You can manually activate the license for a firewall connected to the Internet, or a firewall on an isolated network. You can also use the following processes to relicense a firewall. If at any time you change the terms of your support contract, purchase additional features, or perform a major version upgrade, you must relicense your system.



Note: If you relicense to a new system ID, you must call technical support.

License a firewall connected to the Internet

If your firewall is connected to the Internet, you can license it from the Admin Console.

Steps

- 1) Locate the serial number for your firewall using the information on the *Quick Start Wizard Response Form* you completed earlier.
- 2) In the Admin Console, select **Maintenance > License**. The **License** window appears.



Tip: For option descriptions, click **Help**.

- 3) Click the **Contact** tab, and enter your company contact information.
- 4) Click the **Company** tab, and enter your company information.
- 5) Click the **Firewall** tab, and enter the firewall information:
 - a) **Serial Number** — Type the 16-digit alphanumeric serial number for this firewall.
 - b) **System ID** — Accept the default.



Note: Do not change the system ID unless instructed by technical support.

- 6) Click **Activate firewall**. The firewall uses an encrypted HTTPS session to send the license information to the licensing website.
If the data is complete, a new activation key code appears in the **Activation Key** field. The **Current Features** list updates with the new license information.
Your firewall software and any features you licensed are activated.

Related concepts

[Planning your setup](#) on page 21

Related tasks

[Configure the license tabs](#) on page 59

License a firewall on an isolated network

If you are on an isolated network and do not have access to the activation server, you can activate your license from a computer that has Internet access.

After activating the license and saving the activation key, use the Admin Console to import the activation key into the firewall.

Obtain an activation key

License a firewall on an isolated network.

Steps

- 1) On the Admin Console, select **Maintenance > License**. The **License** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click the **Firewall** tab.
 - a) **Serial Number** — Verify that the 16-digit alphanumeric serial number matches the serial number on the *Quick Start Wizard Response Form* you completed earlier.
 - b) **System ID** — Accept the default.



Note: Do not change the system ID unless instructed by technical support.

- 3) [Conditional] If your Admin Console computer does not have Internet access, move to a computer that has access. You will need:
 - Serial number
 - System ID
- 4) Open a web browser, and navigate to <http://sidewinder.activations.forcepoint.com>.
- 5) Browse to the Forcepoint Sidewinder activation page.
- 6) Complete the form on the website, and click **Submit**. A confirmation screen appears.
- 7) Verify that the information you entered is correct.



Tip: If you want to make changes, use the **Back** button to return to the form.

- 8) Click **Submit**. After approximately one minute, a new webpage appears displaying the activation key.
- 9) Follow the on-screen instructions to save the activation key to a USB drive.



Tip: You can continue following the on-screen instructions to import the file using command line or the Admin Console.

Related reference

[Quick Start Wizard Response Form](#) on page 38

Import the activation key into the firewall

Import the activation key from a USB drive.

Steps

- 1) Insert the USB drive into the Admin Console computer.
- 2) Select **Maintenance > License**. The **License** window appears.



Tip: For option descriptions, click **Help**.

- 3) Click the **Firewall** tab.
- 4) Click **Import Key**. The **Import Key** window appears.
- 5) Complete the information.
 - a) Select **Local File**.
 - b) Enter the file name, or click **Browse** and navigate to the file.
- 6) Click **OK**. The activation key is extracted from the file, and it appears in the **Activation Key** field. Your firewall software and any features you licensed are activated.

Related tasks

[Run the Quick Start Wizard](#) on page 45

[Configure the license tabs](#) on page 59

Configure the license tabs

Configure licensing information on the tabs on the **License** window.

Configure the Contact tab

Configure license information for the **Contact** tab.

Steps

- 1) Select **Maintenance > License**. The **License** window appears.
- 2) Click the **Contact** tab, and enter the contact information.

- 3) From the toolbar, click **Save**.



Tip: For option descriptions, click **Help**.

Configure the Company tab

Configure license information for the **Company** tab.

Steps

- 1) Select **Maintenance > License**. The **License** window appears.
- 2) Click the **Company** tab.



Tip: For option descriptions, click **Help**.

- 3) Click the **Company Address** tab, and complete the information.
- 4) Click the **Billing Address** tab, and complete the information.
- 5) From the toolbar, click **Save**.

Configure the Firewall tab

Configure license information for the **Firewall** tab.

Steps

- 1) Select **Maintenance > License**. The **License** window appears.
- 2) Click the **Firewall** tab.



Tip: For option descriptions, click **Help**.

- 3) [Conditional] If you are manually activating a license or relicensing a firewall, verify that the 16-digit alphanumeric serial number matches the serial number on the Activation Certificate or the appliance.
- 4) In the **System ID** field, accept the default.



Note: Do not change the system ID unless instructed by technical support.


Related tasks

[Manually activate a license on page 57](#)

Complete post-setup tasks

Perform additional tasks that, depending on your site configuration, might be beneficial starting points for implementing your policy.

Table 8: Post-setup tasks

Task	Description	Related topics
Check for updates and patches.	If you have a support contract, set your firewall to automatically load and install available patches. You can check for patches manually or check our website periodically for available patches and other technical support information.	<i>General maintenance</i> http://sidewinder.downloads.forcepoint.com
Configure rule elements, access control rules and groups, and SSL rules.	Access control rules determine which network flows are allowed and denied, and SSL rules determine if the firewall inspects SSL connections.	<i>Policy overview</i> <i>Network objects and time periods</i> <i>Identity validation</i> <i>Content inspection</i> <i>Applications</i> <i>Application Defenses</i> <i>Content inspection</i> <i>Access control rules</i> <i>SSL rules</i>
Set up accounts for other administrators.	You might need more than one administrator account on the system if your site divides administrative tasks among several administrators.	<i>General maintenance</i>
Reconfigure DNS to Firewall Hosted.	Using hosted DNS places the DNS servers on the firewall's hardened operating system, which helps prevent any attacks against these servers from penetrating your network.	<i>DNS (domain name system)</i>
Configure your internal mail server to route email through the firewall.	How you do this depends on the email software you use internally. Note: <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> Note: If your routing directs outbound mail to the firewall, you do not need any additional configuration of your internal mail server.</p> </div>	Check your mail server documentation for help.

Task	Description	Related topics
Run Reconfigure Mail.	<p>Configure your basic mail services using the Reconfigure Mail tool. After configuration is complete, create the necessary objects and access control rules.</p> <ul style="list-style-type: none"> • Transparent — With this selection: <ul style="list-style-type: none"> • Create two access control rules—one for inbound mail and one for outbound mail. • Use the SMTP application. • Use two Mail (SMTP proxy) application defenses—one for inbound traffic and one for outbound traffic, each with direction-appropriate settings. • Secure Split SMTP Servers — With this selection: <ul style="list-style-type: none"> • Create two access control rules—one for inbound mail and one for outbound mail. • Use the Sendmail Server application. • For each rule, make sure: <ul style="list-style-type: none"> • Destination zone is <Any> • Destination endpoint is <Any> • Use two Mail (Sendmail) application defenses—one for inbound traffic and one for outbound traffic, each with direction-appropriate settings. 	<i>Email</i>
Set up an authentication server to validate remote users.	You might need to register the firewall with that server and perform additional steps.	<i>Identity validation</i>
Set the date and time.	Accurate date and time are important for audit records and time-dependent access control rules.	<i>General maintenance</i>
Create a configuration backup.	<p>An initial configuration backup is automatically created when you first configure your firewall. If you have made changes, now is a good time to create another configuration backup. Backing up the configuration files lets you quickly restore a firewall to its desired operational state. By storing your configuration, you can:</p> <ul style="list-style-type: none"> • Back up your initial configuration. • Quickly reconfigure your system after a hardware failure. 	

Task	Description	Related topics
Complete your audit management setup.	Complete the setup, then test it to make sure you are getting the results you intend. Once setup is complete, log files transfer and roll automatically, giving you the audit data you need and keeping the firewall running freely.	<i>Managing log files</i>

Related concepts

[Applications](#) on page 70

[Managing log files](#) on page 309

PART II

Policy

Contents

- [Policy overview](#) on page 67
- [Network objects and time periods](#) on page 85
- [Identity validation](#) on page 93
- [Content inspection](#) on page 113
- [McAfee EIA](#) on page 147
- [Applications](#) on page 165
- [Application Defenses](#) on page 179
- [Access control rules](#) on page 197
- [SSL rules](#) on page 213
- [Policy in action](#) on page 223

Policy overview

Contents

- [Types of rules](#) on page 67
- [What access control rules do](#) on page 68
- [Logic of SSL rules](#) on page 73
- [Interaction between rule types](#) on page 80
- [Rule order](#) on page 81

Rules provide the means for applying Sidewinder policy — they determine how the firewall processes network traffic.

Types of rules

There are two types of rules — *access control rules* and *SSL rules*.

- **Access control rules** — Enforce policy on connections that attempt to pass through or connect to the firewall.
- **SSL rules** — Determine whether the firewall decrypts SSL connections.

The firewall examines both types of rules for each new connection.

Rules are defined using the following types of elements:

- **Condition** — Determine if a connection matches a rule.
- **Action** — Specify how a rule processes a connection.

Rule order is important because Sidewinder searches the enabled rules in sequential order, and rules are applied on a first-match basis.

Related concepts

[Interaction between rule types](#) on page 80

[Rule order](#) on page 81

[Configuring SSL rules](#) on page 213

Related information

[Creating and managing access control rules](#) on page 197

[Working with policy](#) on page 223

What access control rules do

Access control rules enforce policy on network flows that attempt to pass through or connect to the firewall. All network flows that do not match a rule are denied.

Related concepts

- [Types of access control rules](#) on page 68
- [Access control rule elements](#) on page 69
- [Interaction between rule types](#) on page 80
- [Rule order](#) on page 81

Types of access control rules

There are two types of access control rules.

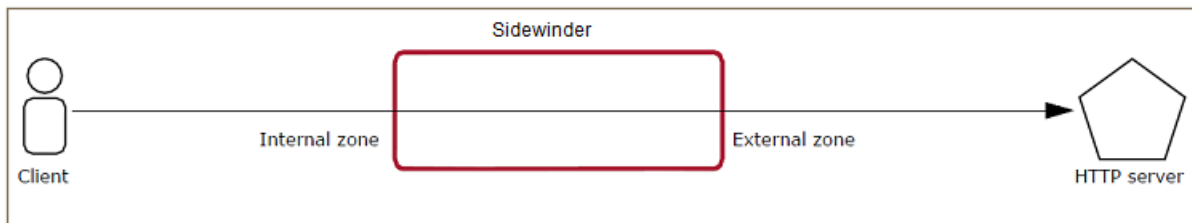
- Allow rules
- Deny and drop rules

Allow rules

Allow rules permit a connection to proceed to its destination after the firewall inspects it.

In the figure below, an internal client connects to an external HTTP server. For this connection to succeed, it must match an allow rule.

Figure 15: Allowed connection



The following rule would allow the connection shown in the table below.

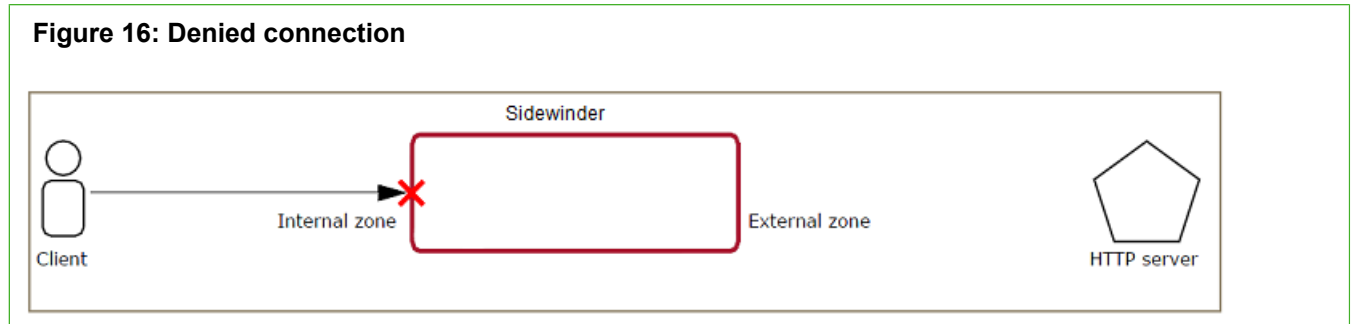
Table 9: Outbound allow rule

Option	Selection
Action: Allow	Application: HTTP
Source zone: internal	Destination zone: external
Source endpoint: Any	Destination endpoint: Any
NAT address: localhost	Redirect: None

Deny and drop rules

Deny and drop rules prevent a connection from reaching its destination. A deny rule notifies the sender that the request was rejected while a drop rule does not.

In the figure below, an internal client attempts to connect to an external HTTP server, but the firewall denies the connection.



The following rule causes the firewall to deny the connection.



Tip: A connection is also denied if it does not match any of the active allow rules.

Table 10: Outbound deny rule

Action: Deny	Application: HTTP
Source zone: internal	Destination zone: external
Source endpoint: <Any>	Destination endpoint: <Any>
NAT address: <localhost>	Redirect: <None>

Access control rule elements

Access control rules are defined using *Condition elements* and *Types of Action elements*.

- **Condition elements** — Determine if a connection matches a rule
- **Types of Action elements** — Specify how a rule processes a connection

Table 11: Rule element processing

Does the connection match the condition elements?	Result
Yes	The rule handles the connection according to the specified action elements
No	The connection passes to the next rule

The following sections describe these rule elements and provide an overview of how to use them in a rule.

Condition elements for access control rules

Sidewinder examines the condition elements specified on a rule to determine if a connection matches that rule. The condition elements are as follows.

Applications

We have an extensive list of applications that classify network flows based on function. To specify which network applications are managed by an access control rule, select one or more applications.

Each application identifies the following, which simplifies administration:

- Ports
- Protocols
- Signatures

Customize the application or tailor the access control rule to meet your needs.

Related information

[Using applications in policy](#) on page 165

Source and destination

A rule matches the source and destination of a connection based on the specified endpoints, zones, and user groups.

Table 12: Source and destination elements

Element	Description
Endpoints	<p>Match the source and destination of a connection based on the network identity of the source or destination host.</p> <p>Use network objects to specify endpoints. Network objects identify hosts based on network attributes such as IP address or host name.</p> <ul style="list-style-type: none"> • Source endpoints are specified using network objects, which define the identity of a host using network characteristics, such as an IP address or host name. • Destination endpoints are specified using network objects and SmartFilter URL categories.
Zones	<p>Match the network region that contains the endpoint .</p> <ul style="list-style-type: none"> • A rule can reference a single zone, multiple zones, or a zone group. • If no endpoints are specified, all endpoints in the specified zone are allowed.

Element	Description
User groups	<p>Match the source of a connection based on the identity of the user that is logged on to the initiating host.</p> <p>Specify users and user groups as source attributes of SSL rules. User identity is established using two types of identity verification:</p> <ul style="list-style-type: none"> • Passive — If your organization uses Microsoft Active Directory, each user is defined in an Active Directory object. The firewall monitors the authentication status, group membership, and current IP address of each user by communicating with the McAfee Logon Collector agent, which is installed on a Windows server. Users are not prompted for authentication by the firewall. • Active — The firewall prompts users to provide credentials.

Global Threat Intelligence

McAfee Global Threat Intelligence is an Internet reputation service that assigns a reputation score to an IP address based on the behavior attributes of the traffic it generates.

A reputation score is like a credit score that indicates the trustworthiness of an IP address. When enabled on a rule, Global Threat Intelligence matches the source or destination of a connection based on the specified reputation categories.

Time Periods

Time periods determine the segment of time a rule is in effect.

Time periods can be recurring, making the rule active for the same time on the same day every week, or continuous, making the rule active one time only.

The lifetime of a rule can also be controlled by delaying the start time and scheduling an end time.

Types of Action elements

Action elements determine how the firewall processes a connection if it matches a rule.

The action elements are:

- Action
- NAT
- Redirect
- Audit
- Intrusion Prevention System (IPS)
- Application Defenses

Action

The action determines how a rule primarily processes a matching connection.

The actions are:

- **Allow** — Permits the connection to continue to its destination.
- **Deny** — Prevents the connection from going through the firewall and sends the source a message that the request was rejected.

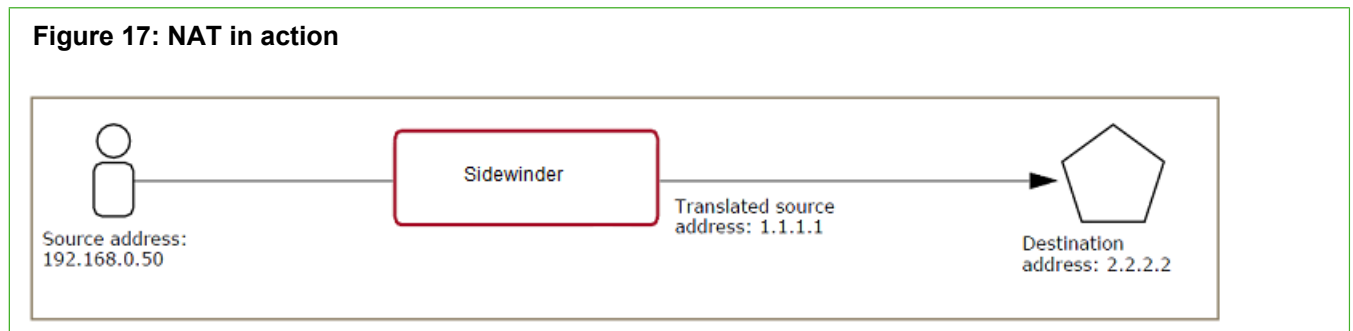
- **Drop** — Prevents the connection from going through the firewall without notifying the source.

NAT

Network address translation (NAT) replaces the source IP address of a connection with a new source IP address. NAT is enabled on an access control rule by selecting a network object or `<localhost>`, which uses the firewall's IP address in the destination zone.

NAT is commonly used to allow hosts in a private address space to communicate with hosts in a public network.

In the example illustrated below, an internal host (192.168.0.50) initiates a connection to an external host (2.2.2.2). Because the source host has a private IP address, the firewall changes the source IP to its own external IP address (1.1.1.1) using NAT.



The outbound access control rule must translate the internal host address to the firewall's external address.

Table 13: Outbound NAT rule

Source zone: internal	Destination zone: external
Source endpoint: 192.168.0.50 (internal host)	Destination endpoint: 2.2.2.2 (destination host)
NAT: <code><localhost></code>	Redirect: <code><None></code>

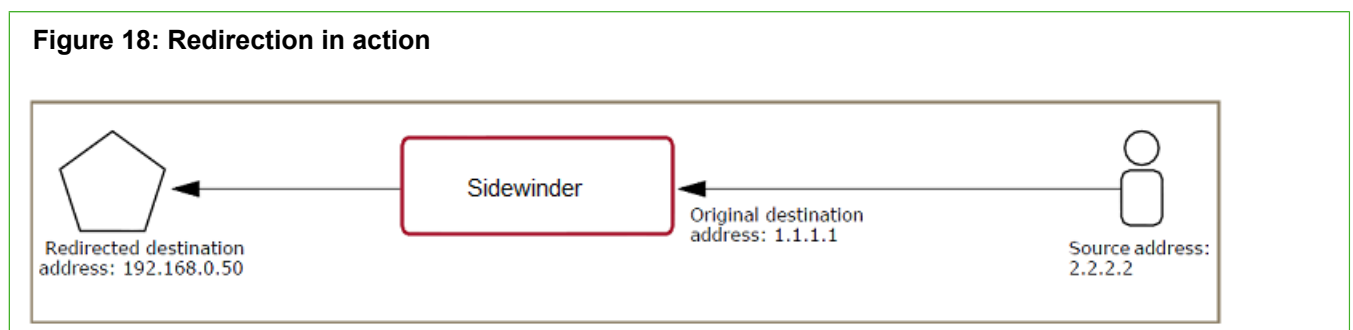


Note: In an audit entry for a rule using NAT, the source IP is the original source IP. The NAT address does not appear in the audit.

Redirect

Redirection replaces the destination IP of a connection with a new destination address. A redirect is enabled on an access control rule by selecting a network object.

In the figure below, an external client (2.2.2.2) initiates a connection to the Sidewinder external IP address (1.1.1.1). The firewall redirects the connection to the appropriate internal server (192.168.0.50).



The inbound access control rule must redirect the connection to the internal host.

Table 14: Inbound redirect rule

Source zone: external	Destination zone: external
Source endpoint: 2.2.2.2 (external client)	Destination endpoint: 1.1.1.1 (external firewall address)
NAT address: <None>	Redirect: 192.168.0.50 (internal server)

Audit

Audit levels determine how much audit data a rule generates. By default, all rules generate connection data that includes the connection's source, destination, and application. The amount of audit data generated can be increased to aid in troubleshooting or decreased to include errors only.

Intrusion Prevention System (IPS)

The IPS area consists of both a signature group and a response mapping. The signature group identifies which signatures of known network-based intrusion attacks to compare to the connection. The response mappings indicate what to do if an attack is recognized.

Available response mappings are:

- Allow
- Deny
- Drop
- Blackhole

Application Defenses

Application Defenses determine application-specific constraints and filtering actions.

- **Protocol enforcement** — Enforces RFC (Request for Comments) standards and allowed parameters; configurable parameters include headers, commands, versions, and file sizes
- **Connection settings** — Control timeouts, request and response rates, error and control messages, and the audit rate
- **Virus protection** — Scans connections for viruses and spyware
- **SmartFilter web filtering** — Filters HTTP-based applications

Logic of SSL rules

SSL rules determine whether the firewall decrypts SSL connections. Regardless of an SSL rule match, SSL connections must match an access control rule to pass through the firewall.

Use an SSL rule when you want to identify and inspect SSL-encapsulated applications.




Tip: Applications that use SSL include SSL ports (example: SSL/443).

Types of SSL rules

Available rule actions vary depending on the selected SSL rule type.

Table 15: SSL rule types and actions

SSL rule type	Available SSL rule actions
<Any> — Exempts matching connections from decryption regardless of whether they are inbound or outbound	No decryption — Exempts the connection from matching subsequent SSL rules
Outbound — Protects clients behind the firewall	<ul style="list-style-type: none"> No decryption — Exempts the connection from matching subsequent SSL rules Decrypt/re-encrypt — Decrypts the connection so the content can be inspected, then re-encrypts it
Inbound — Protects servers behind the firewall	<ul style="list-style-type: none"> No decryption — Exempts the connection from matching subsequent SSL rules Decrypt only — Decrypts the connection so the content can be inspected <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p> Note: The connection leaves the firewall decrypted.</p> </div> <ul style="list-style-type: none"> Decrypt/re-encrypt — Decrypts the connection so the content can be inspected, then re-encrypts it

Outbound SSL rules

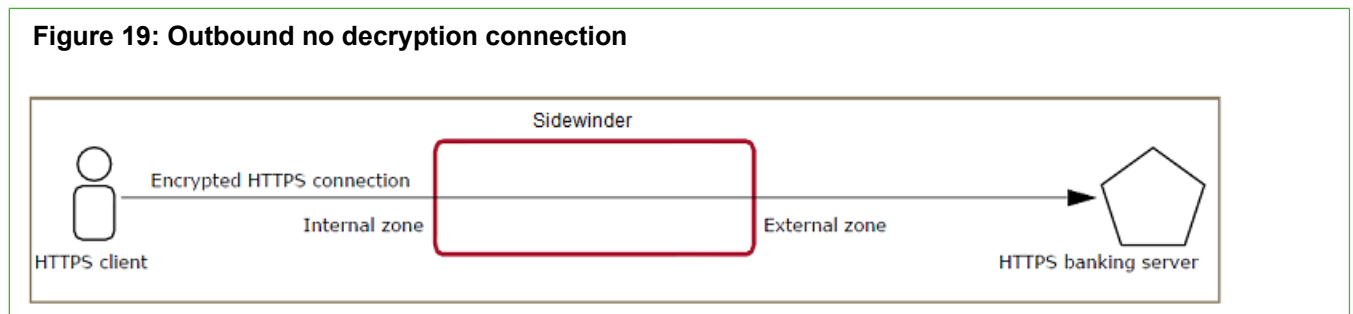
Outbound SSL rules process encryption for SSL connections that originate from clients protected by the firewall.

Two actions are available:

No decryption for outbound connections

No decryption SSL rules exempt outbound connections from matching subsequent SSL rules.

In the figure below, an internal client connects to an external HTTPS banking server. The connection remains encrypted from end to end.



Tip: The SSL rule below is required only if you need to exempt the connection from matching a subsequent decrypting SSL rule.

Table 16: Required rules

Access control rule		SSL rule	
Action: Allow	Application: SSL/TLS	Type: Outbound	
Source zone: internal	Destination zone: external	Action: No decryption	Port: <Any> or 443
Source endpoint: <Any>	Destination endpoint: <Any>	Source zone: internal	Destination zone: external
NAT: <localhost>	Redirect: <None>	Source endpoint: <Any>	Destination endpoint: Finance/Banking (URL category)



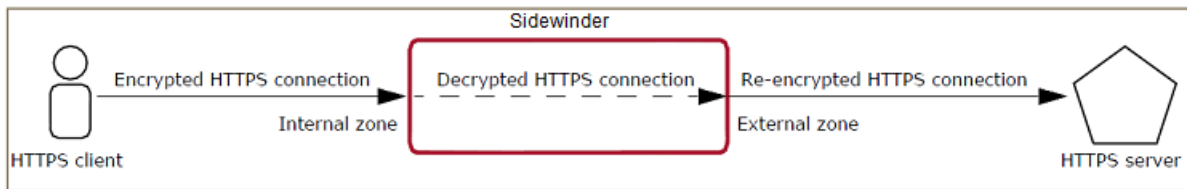
Note: The example rules above illustrate one of several ways to achieve this outcome.

Decrypt/re-encrypt for outbound connections

Decrypt/re-encrypt SSL rules decrypt matching connections to perform SSL content inspection. Before the connection leaves the firewall, it is re-encrypted.

In the figure below, an internal client connects to an external server. The firewall decrypts the connection, inspects it, re-encrypts it, then forwards the encrypted connection to the server.

Figure 20: Outbound decrypt/re-encrypt connection



The following rules are required to take the action shown in the table below.



Tip: To avoid certificate errors, the clients must trust the firewall CA certificate.

Table 17: Required rules

Access control rule		SSL rule	
Action: Allow	Application: HTTP or SSL/TLS	Type: Outbound	
Source zone: internal	Destination zone: external	Action: Decrypt/re-encrypt	Port: <Any> or 443
Source endpoint: <Any>	Destination endpoint: <Any>	Source zone: internal	Destination zone: external
NAT: <localhost>	Redirect: <None>	Source endpoint: <Any>	Destination endpoint: <Any>



Note: The example rules above illustrate one of several ways to achieve this outcome.

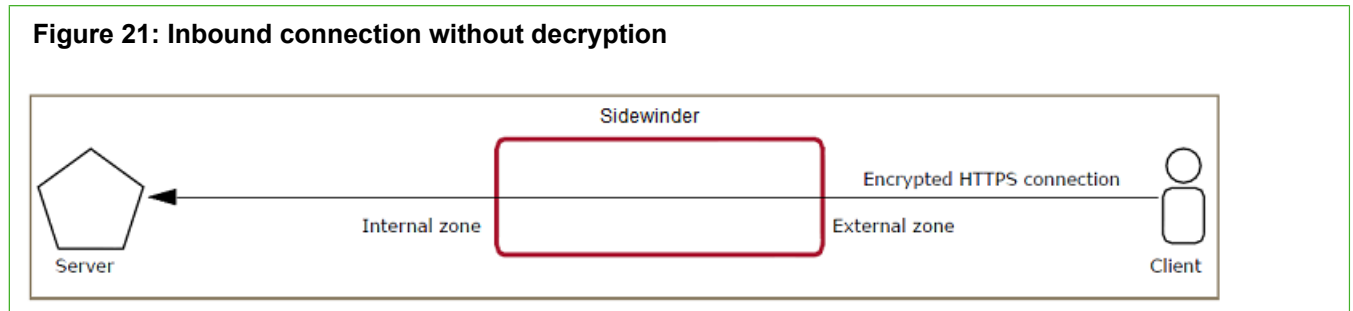
Inbound SSL rules

Inbound SSL rules process encryption for SSL connections that are destined for servers protected by the firewall. The following actions are available.

No decryption for inbound connections

No decryption SSL rules exempt inbound connections from matching subsequent SSL rules.

In the figure below, an external client connects to the firewall external IP address and is redirected to an internal server. The connection remains encrypted from end to end.



The following rules are required to take the action shown in the following figure.



Tip: The SSL rule below is required only if you need to exempt the connection from matching a subsequent SSL rule.

Table 18: Required rules

Access control rule		SSL rule	
Action: Allow	Application: SSL/TLS	Type: Inbound	
Source zone: external	Destination zone: external	Action: No decryption	Port: <Any> or 443
Source endpoint: <Any>	Destination endpoint: Firewall external IP	Source zone: external	Destination zone: external
NAT: <None>	Redirect: Server IP	Source endpoint: <Any>	Destination endpoint: <Any>



Note: The example rules above illustrate one of several ways to achieve this outcome.

Decrypt only

Decrypt only SSL rules decrypt matching connections to perform SSL content inspection. When the connection leaves the firewall, it remains decrypted.

In the figure below, an external client connects to the firewall external IP address and is redirected to an internal server. The firewall decrypts the connection, inspects it, then redirects the decrypted connection to the server on port 80.

Figure 22: Inbound connection with decryption



The following rules are required to take the action shown in the table below.

Table 19: Required rules

Access control rule		SSL rule	
Action: Allow	Application: HTTP or SSL/TLS	Type: Inbound	
Source zone: external	Destination zone: external	Action: Decrypt only	Port: <Any> or 443
Source endpoint: <Any>	Destination endpoint: Firewall external IP	Source zone: external	Destination zone: external
NAT: <None>	Redirect:: Server IP Redirect port: 80	Source endpoint: <Any>	Destination endpoint: <Any>

Decrypt/re-encrypt for inbound connections

Decrypt/re-encrypt SSL rules decrypt matching connections to perform SSL content inspection. Before the connection leaves the firewall, it is re-encrypted.

In the figure below, an external client connects to the firewall external IP address and is redirected to an internal server. The firewall decrypts the connection, inspects it, re-encrypts it, then redirects the encrypted connection to the server.

Figure 23: Inbound connection with decryption and re-encryption



The following rules are required to take the action shown in the table below.

Table 20: Required rules

Access control rule		SSL rule	
Action: Allow	Application: HTTP or SSL/TLS	Type: Inbound	
Source zone: external	Destination zone: external	Action: Decrypt/re-encrypt	Port: <Any> or 443

Access control rule		SSL rule	
Source endpoint: <Any>	Destination endpoint: firewall external IP	Source zone: external	Destination zone: external
NAT: <None>	Redirect: Server IP	Source endpoint: <Any>	Destination endpoint: <Any>



Note: The example rules above illustrate one of several ways to achieve this outcome.

SSL rule elements

SSL rules are defined using Condition and Action elements.

- **Condition elements** — Determine if a connection matches a rule
- **Action element** — Specifies how a rule processes a connection

Table 21: SSL rule element processing

Does the connection match the condition elements?	Result
Yes	The rule handles the connection according to the specified action elements
No	The connection passes to the next rule

Condition elements for SSL rules

Sidewinder examines the condition elements specified on an SSL rule to determine if an SSL connection matches that rule.

- SSL rules only match SSL connections.
- Non-SSL connections are not examined.

Ports

An SSL rule matches the destination port of a connection based on the specified TCP ports.

Source and destination

A rule matches the source and destination of a connection based on the specified endpoints, zones, and users.

Table 22: Source and destination elements

Element	Description
Endpoints	Match the source and destination of a connection based on the network address of the source or destination host. Use network objects to specify endpoints. Network objects identify hosts based on network attributes such as IP address or host name.

Element	Description
Zones	<p>Match the network region that contains the endpoint.</p> <ul style="list-style-type: none"> • A rule can reference a single zone, multiple zones, or a zone group. • If no endpoints are specified, all endpoints in the specified zone are allowed.
Users and groups	<p>Match the source of a connection based on the identity of the user that is logged on to the initiating host. Specify users and user groups as source attributes of access control rules. User identity is established using two types of identity verification:</p> <ul style="list-style-type: none"> • Passive — If your organization uses Microsoft Active Directory, each user is defined in an Active Directory object. The firewall monitors the authentication status, group membership, and current IP address of each user by communicating with the McAfee Logon Collector agent, which is installed on a Windows server. Users are not prompted for authentication by the firewall. • Active — The firewall prompts users to provide credentials.

Action element for SSL rules

The action determines how a rule primarily processes a matching connection.

- **No decryption** — Exempts the connection from matching subsequent SSL rules; the connection remains encrypted
- **Decrypt only** — Decrypts the connection so the content can be inspected

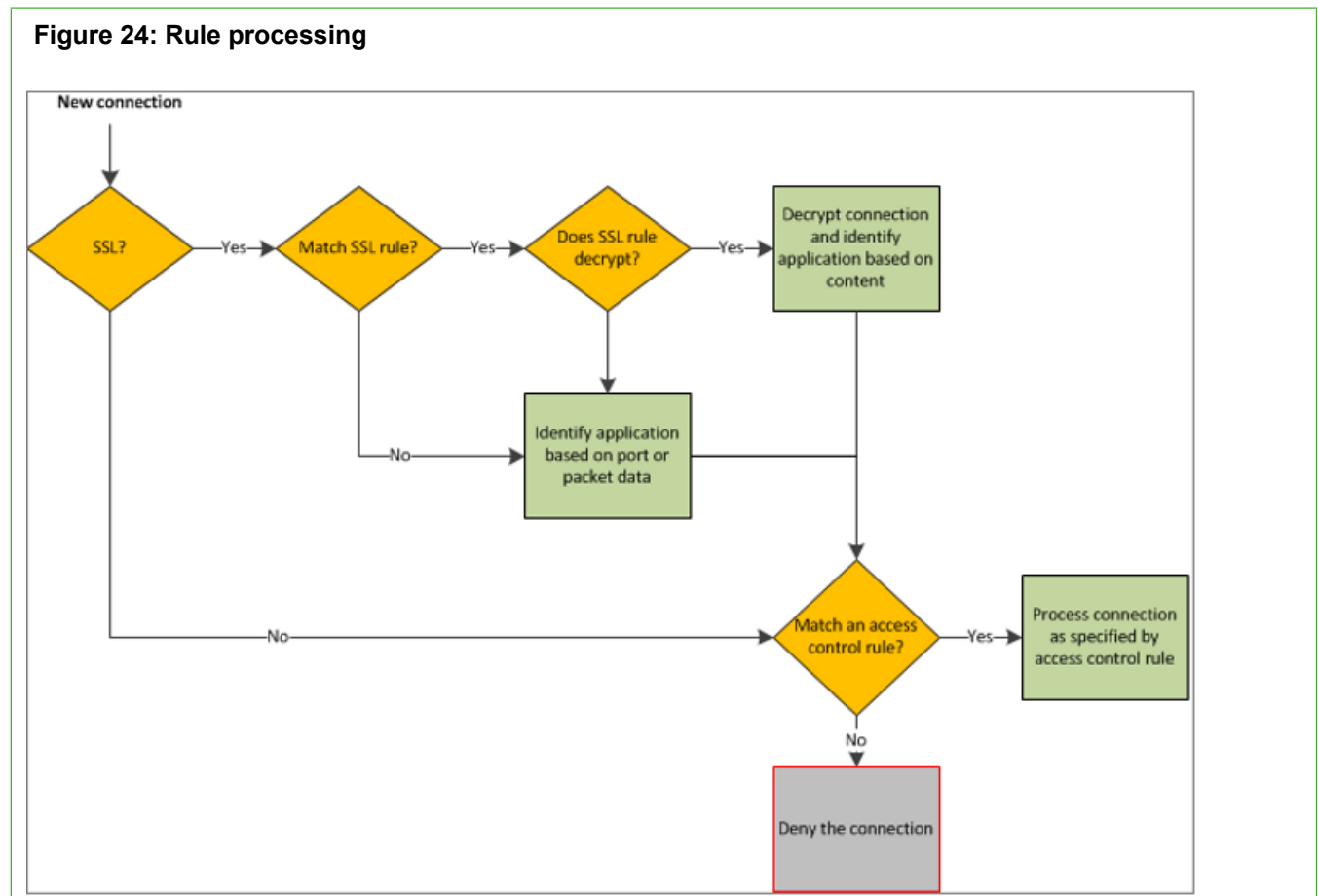


Note: The connection leaves the firewall decrypted.

- **Decrypt/re-encrypt** — Decrypts the connection so the content can be inspected, then re-encrypts it

Interaction between rule types

When the firewall processes a new connection, it checks access control rules and SSL rules as shown by the figure below.



Because SSL connections are encrypted, decryption is required to fully identify the applications used in SSL connections.

- If an SSL connection is decrypted by an SSL rule, the content of the connection is examined to identify the application.
- If an SSL connection is not decrypted by an SSL rule, the application must be identified without examining the connection content.
- In some cases, the application can be identified based on other factors such as port or packet data.
- If no identifying factors are available, the application is identified as SSL/TLS.

The access control rule that matches the SSL connection must take into account whether the connection was decrypted by an SSL rule, since decryption allows the application to be more accurately identified. For example, consider how an access control rule to allow HTTPS connections changes if the connection is decrypted.

Table 23: Rules to allow HTTPS connections

Decrypted by SSL rule?	Application identified as...	Application required on access control rule
Yes	HTTP	Several options are available: <ul style="list-style-type: none"> • SSL/TLS — Matches all applications inside the SSL connection • HTTP — Matches only HTTP-based applications inside the SSL connection • HTTP-based application — Matches only that specific application inside the SSL connection (for example: Facebook)
No	SSL/TLS	SSL/TLS



Note: If the access control rule that matches the SSL connection specifies an Application Defense group that does not assign an HTTP Application Defense (for example: the connections settings group initially specified as the **<Default Group>**), the following SSL rule Decrypt/ Re-encrypt selections are not enforced: **Display notification to web browser** and **Perform certificate hostname matching**.

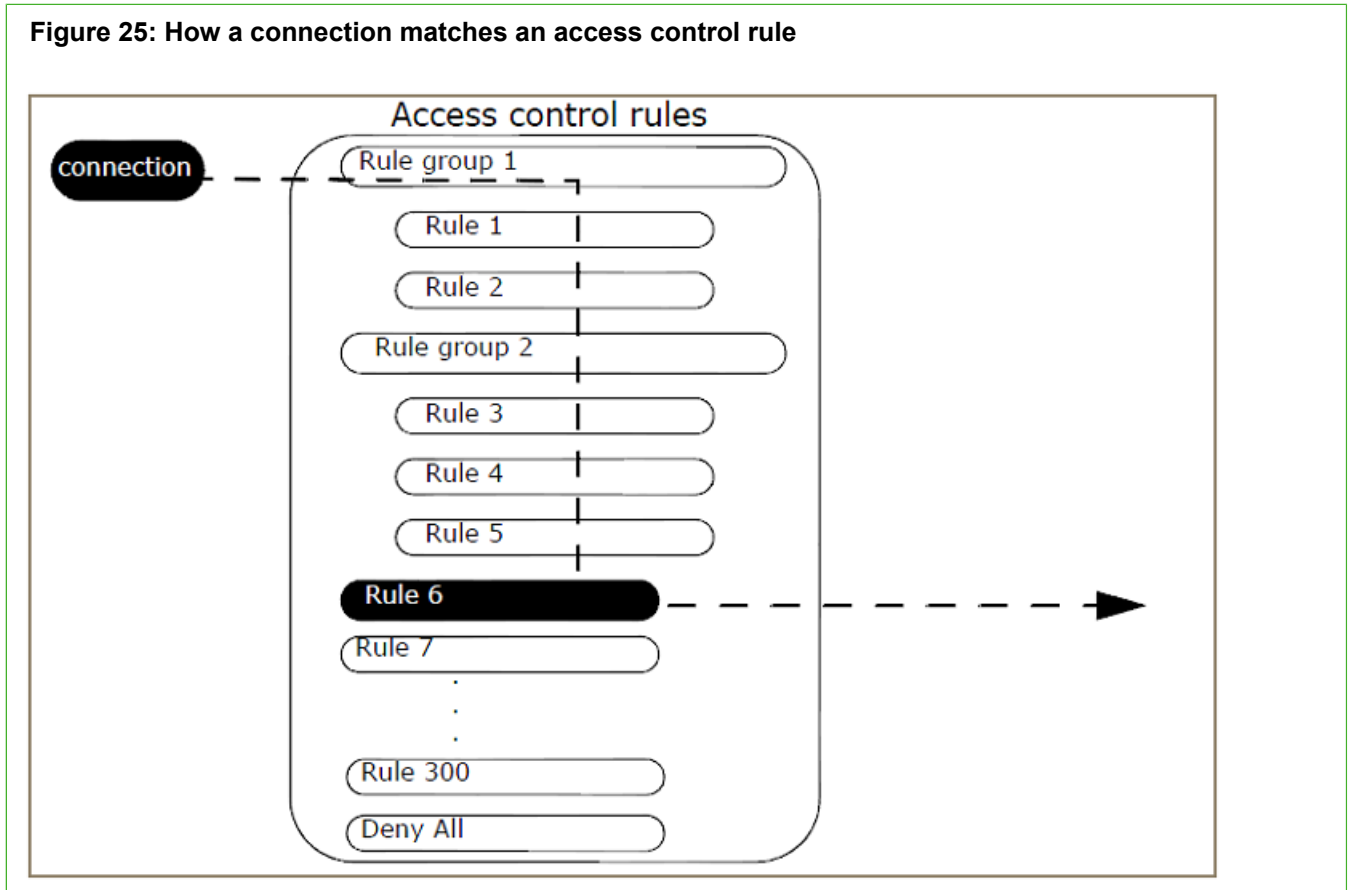
Rule order

The order in which access control rules and SSL rules appear in your policy is significant.

When the firewall receives a connection, it searches the enabled rules in sequential order. If the connection does not match the condition elements of the first rule, it forwards to the next rule. The first rule that matches the connection manages the connection. Once a rule matches, the rule processes the connection based on the configured action elements, and the search stops.

The following figure depicts first-match processing for access control rules.

Figure 25: How a connection matches an access control rule



Rule placement

Place specific rules before general rules.

For example, if you want to deny access to social networking applications and allow web browsing, put the rule to deny social networking before the rule that allows web browsing.

Both the access control rule list and the SSL rule list contain a final default rule that indicates how the firewall processes connections that do not match a previous rule.

Table 24: Default last rule for access control and SSL rule lists

Rule list	Default last rule	Rule purpose
Access control rules	Deny All	All connections that reach it are denied; even if the rule is deleted, the firewall denies connections that do not match an access control rule.
SSL rules	Exempt All	All connections that reach it are exempted from decryption; even if the rule is deleted, connections that do not match an SSL rule are exempted from decryption.



CAUTION: Do not disable or delete the logon rules located in the **Administration** rule group or place them below the **Deny All** rule.

Scenario for ordering access control rules

Suppose you want to deny access to Facebook and allow access to all other HTTP-based applications. The scenarios below illustrate correct and incorrect access control rule placement.

- **Correct rule order** — To deny a particular application, place the deny rule *before* the allow rule.

Table 25: Correct rule placement

Rule 1:	Deny Facebook for all internal systems to all external systems.
Rule 2:	Allow HTTP for all internal systems to all external systems.

- **Incorrect rule order** — The following table shows a rule order that is *incorrect* for this scenario.

Table 26: Incorrect rule placement

Rule 1:	Allow HTTP for all internal systems to all external systems.
Rule 2:	Deny Facebook for all internal systems to all external systems.

Problem: When an internal system attempts to connect to Facebook, the firewall checks rule 1. Because that rule allows access to all HTTP-based applications, the firewall detects a match, stops searching the rules, and grants the connection.

Network objects and time periods

Contents

- [Types of network objects](#) on page 85
- [Manage network objects](#) on page 86
- [Manage netgroup membership](#) on page 89
- [Manage time periods](#) on page 90

Network objects can be used as endpoints in access control and SSL rules. Use network objects to simplify rule creation.

A network object is the source or destination of a connection to or through the Sidewinder appliance.

Types of network objects

A network object can be any of these types.

- **IP address** — Specifies an IP address. Use an IP address network object in a rule to allow or deny a network connection based on the source or destination IP address.
- **IP range** — Specifies a range of IP addresses. Use an IP range network object in a rule to allow or deny a network connection based on a range of a source or destination IP addresses.
- **Subnet** — Specifies an IP address subnet. Use a subnet network object in a rule to allow or deny a network connection based on the subnet of source or destination IP address.
- **Netmap** — Maps multiple IP addresses and subnets to alternate addresses. A netmap network object removes the need to create numerous rules.

A netmap consists of one or more netmap members. A netmap member is any IP address or subnet that you add to a netmap. Each member in the netmap is mapped to an alternate address or subnet that you specify.

- **Domain** — Specifies a domain. Use a domain network object in a rule to allow or deny a network connection based on the source or destination domain.
Domain objects have features that set them apart from other network objects. Before using domain objects in rules, note the following:
 - Domains are dependent on DNS. Because DNS is beyond administrator control, the use of domain network objects can be a security risk.
 - Domain objects require a DNS lookup each time they are used. These DNS lookups can slow performance.



Note: IP filtering does not work on rules that follow a rule that uses a domain object. Rules that follow will be processed using proxies.

- **Host** — Specifies a host name. Use a host network object in a rule to allow or deny a network connection based on the source or destination host.



Note: In IP filter rules, the localhost network object is supported, but DNS-resolvable host names should be avoided. DNS-resolvable host names become inoperative during any periods when the appropriate DNS server is unavailable or unreachable.

- **Geo-Location** — Specifies the country of origin of an IP address. More than one country can be included in a single Geo-Location network object. Use a Geo-Location network object in a rule to allow or deny a network connection based on source or destination countries.



Note: Periodically update the Geo-Location database to ensure that you have the latest country database.

- **Netgroup** — Groups multiple network objects into a single network object. Use a netgroup network object to reference multiple network objects in a single rule.



Tip: You might find it more convenient to create all of your network objects before defining your netgroup objects. That way, as you set up your netgroup objects, you will be able to immediately assign the desired network objects to the group.

Related tasks

[Manage service updates](#) on page 600

Manage network objects

View, create, and maintain network objects.

Steps


- 1) Select **Policy > Rule Elements > Network Objects**. The **Network Objects** window appears.



Tip: For option descriptions, click **Help**.

This window lists the network objects currently configured on the Sidewinder.

- 2) Use the toolbar to perform the listed tasks.

Task	Steps
Create a network object	<ol style="list-style-type: none"> 1) Click New. 2) Select an object from the drop-down menu. 3) Configure the selected Network Objects window that appears. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Note: The name you create here is what you will see as endpoints when you create an access control rule or SSL rule. You will not see any of the object's values, so make a descriptive name to ensure that you will recognize it in the rule windows.</p> </div> 4) Click Add.

Task	Steps
Create a netgroup	<ol style="list-style-type: none"> 1) Click New Group. The Netgroup window appears. 2) Configure the Network Objects: Netgroup window. 3) Click Add.

Task	Steps
Modify an existing network object or netgroup	<ol style="list-style-type: none"> 1) Select the object from the list. 2) Click Modify. 3) Make your changes in the Network Objects window. 4) Click OK. <p>(Read-only administrators can click View to view a network object or netgroup.)</p>

Task	Steps
View a network objects or netgroup	<ol style="list-style-type: none"> 1) Select the object from the list. 2) Click Modify. <p>(Read-only administrators can click View to view a network object or netgroup.)</p>

Task	Steps
Delete an existing network object or netgroup	<ol style="list-style-type: none"> 1) Select the object from the list. 2) Click Delete. A message appears asking you to confirm the deletion. 3) Click Yes.

Task	Steps
Create a duplicate of an existing network object or netgroup	<ol style="list-style-type: none"> 1) Select the object from the list. 2) Click Duplicate. 3) Change the name and make any desired changes. 4) Click Add.

Task	Steps
Rename a network object or netgroup	<ol style="list-style-type: none"> 1) Select the object from the list. 2) Click Rename. 3) Type the new name in the Network Objects window. 4) Click OK.

Task	Steps
View where a particular network object or netgroup is used	<ol style="list-style-type: none"> 1) Select the object from the list. 2) Click Usage. The Usage window appears listing the netgroups, netmaps, and rules that use the network object or netgroup.

Task	Steps
Delete unused network objects	<ol style="list-style-type: none"> 1) Click Delete unused network objects. The Delete unused objects window appears. 2) Select the objects that you want to delete. 3) Click OK.

Task	Steps
Search for specific elements in the list	Type your search criteria in the Find field. Objects with matching elements appear in the list.
Task	Steps
View or modify the group membership of a network object or netgroup	<ol style="list-style-type: none"> 1) Select the object from the list. 2) Click Groups Object In. The Group Membership window appears. 3) Select the groups to assign the network object to. 4) Click OK.


Manage netgroup membership

Manage the groups that a network object belongs to.

You can modify a group membership in two ways:

- Modify the group:
 - 1) In the **Network Objects** window, select the desired *netgroup* from the list.
 - 2) Click **Modify**.
 - 3) Make the membership changes in the **Netgroup** window.
 - 4) Click **OK**.

- Modify the group member:
 - 1) In the **Network Objects** window, select a *network object* from the list.
 - 2) Click **Groups Object In**. The **Group Membership** window appears.

 **Tip:** For option descriptions, click **Help**.
 - 3) Move groups to and from the **Selected** list.
 - 4) Click **OK**.

Manage time periods

A time period is a rule element that can specify a segment of time a rule is in effect. Time periods can be selected on access control rules.

Use the **Time Periods** window to view, create, and maintain time periods.

Steps

- 1) Select **Policy > Rule Elements > Time Periods**. The **Time Periods** window appears.



Tip: For option descriptions, click **Help**.

- 2) Use the toolbar or the lower pane to perform the listed tasks.

Task	Steps
Create a new time period	<ol style="list-style-type: none"> 1) Click New. The Time Periods: New Time Period window appears. 2) Configure the fields for the new time period. 3) Click Add.

Task	Steps
Modify a time period	<ol style="list-style-type: none"> 1) Select a time period from the list. 2) Do one of the following: <ul style="list-style-type: none"> • Modify the settings in the lower pane. • Click Modify. The Time Periods: Modify Time Period window appears. <ol style="list-style-type: none"> 1) Make your changes. 2) Click OK.

Task	Steps
View a time period	Select a time period from the list. Information about that time period appears in the lower pane.

Task	Steps
Delete a time period	<ol style="list-style-type: none"> 1) Select a time period from the list. 2) Click Delete. A message appears asking you to confirm the deletion. 3) Click Yes.

Task	Steps
Rename a time period	<ol style="list-style-type: none"> 1) Select a time period from the list. 2) Click Rename. The Time Periods: rename window appears. 3) Type a new name. 4) Click OK.
Task	Steps
View which rules are using a time period	<ol style="list-style-type: none"> 1) Select a time period from the list. 2) Click Usage. An Info window appears, listing all the rules that use the selected time period.
Task	Steps
Search for specific elements in the list	Type your search criteria in the Find field. Time periods with matching elements appear in the list.

Identity validation

Contents

- [Validating users and user groups](#) on page 93
- [Passive identity validation](#) on page 94
- [Active identity validation](#) on page 95
- [Users and user groups](#) on page 106

The firewall can validate the identity of matching users trying to gain access. Identity can be validated in a passive or active way.

Validating users and user groups

A user is a person who uses the networking services provided by the firewall. A user group is a logical grouping of one or more users, identified by a single name.

Users and groups can be used as matching elements in access control rules and SSL rules.



Note: Users that do not match a rule are not explicitly denied and could be allowed by a subsequent rule.

The firewall can validate the identity of matching users trying to gain access. Identity can be validated in two ways:

- **Passive** — All user status information is stored on a Microsoft Active Directory server. McAfee Logon Collector gathers this information, and you configure a Passive Passport on the firewall to communicate with McAfee Logon Collector. Users are not prompted for authentication by the firewall.
- **Active** — An authenticator is configured on the firewall, and the firewall prompts users to provide credentials. You can configure an Active Passport so that an authenticated user's source IP address is cached, and subsequent connection attempts are not prompted for authentication.



Tip: You can also use McAfee EIA to collect user and connection information from Windows-based systems.



Note: All IP addresses in identity validation must be IPv4.

This chapter explains how to configure passive and active identity validation, and how to manage users and user groups.

Related concepts

[Passive identity validation](#) on page 94

[Active identity validation](#) on page 95

[Users and user groups](#) on page 106

[How McAfee EIA works](#) on page 147

Passive identity validation

You can use Passive Passport to allow matching users to connect without prompting for authentication.

If your organization uses Microsoft Active Directory, each user is defined as an Active Directory object. The firewall monitors the authentication status, group membership, and current IP address of each user by communicating with the McAfee Logon Collector software, which is installed on a Windows server. Users are authenticated by the Active Directory server. They are not prompted for authentication by the firewall.

The following high-level tasks must be performed to use Passive Passport.

- 1) Define users on an Active Directory server.
- 2) Install McAfee Logon Collector on a Windows server. Refer to the *McAfee Logon Collector Product Guide* for information.
- 3) On the firewall **Passport** window, enable Passive Passport and configure the connection between the firewall and McAfee Logon Collector.
- 4) In the **Rule Properties** window for access control rules or SSL rules, allow connections for selected users and groups based on organizational criteria.

To configure Passive Passport:

- 1) Select **Policy > Rule Elements > Passport**. The **General** tab of the **Passport** window appears.



Tip: For option descriptions, click **Help**.

- 2) Select **Passive (MLC)**.
- 3) Configure the connection between the firewall and McAfee Logon Collector.
 - **IP address** — Enter the address of the server that McAfee Logon Collector is installed on.
 - **Certificate** — The MFE_Communication_Cert certificate is selected by default to identify the firewall to McAfee Logon Collector. You can select your own certificates if you want.



Tip: Click **Test MLC Connection** to verify connectivity with McAfee Logon Collector.

- 4) Click the **Advanced** tab.
- 5) Select the CA that should be used for validation of the McAfee Logon Collector connection:
 - To use the McAfee Logon Collector default self-signed certificate, click **Retrieve MLC Root Cert**.

- To use a previously defined CA, select a CA from the **Cert Authority** drop-down list.
- 6) In the **User cache timeout** field and drop-down list, set the length of time that users and groups are cached on the firewall when not connected to McAfee Logon Collector.
 - 7) Save your changes.

Active identity validation

Active identity validation requires a user to provide a user name and valid password and/or a special passcode or personal identification number (PIN) before being logged on to a server.

To use active identification, configure an authenticator and then do either of the following:

- Configure Active Passport for that authenticator. Active Passport caches the source IP address of an authenticated user for a specified time. Subsequent connection attempts from the same IP address are allowed without prompting for authentication.
- Select the configured authenticator when creating an access control rule. Depending on the authentication method used, a person must provide a user name and valid password and/or a special passcode or personal identification number (PIN) before being logged on to a server.



Note: Active identification cannot be established by an SSL rule. However, users that are first granted an active passport by an access control rule can subsequently match an SSL rule.

Related concepts

[Active Passport configuration](#) on page 95

[Authenticator configuration](#) on page 100

[User password management](#) on page 104

Active Passport configuration

Active Passport associates an authenticated user with their IP address. A Passport is acquired by successfully logging on using a designated authenticator.

- 1) On the **Authenticators** window, you configure authenticators.
- 2) On the **Passport** window, you select authenticators that can be used to acquire an Active Passport.
- 3) Create an access control rule and include the following selections:
 - **Authenticator** — <None/Passport >
 - **Users and Groups** — <Authenticated> or specific users and groups
- 4) After a user successfully authenticates the network connection using a designated authenticator, they acquire an Active Passport and their IP address is cached for a specified time. Subsequent connection attempts from the same IP address are assumed to be from the same authenticated user, and if <None/

Passport> is the authentication method for the rule, the connection is allowed without prompting for authentication.

Active Passports can be revoked in these ways:

- A Passport can expire after a configured time has passed.
- A Passport can expire after a configured idle period.
- An administrator can revoke a Passport directly.

Active Passport options

There are several ways to use Active Passport.

- **Authenticator groups** — You can designate a group of authenticators that can be used to acquire a Passport. If Passport is the authentication method in a rule, any of the selected authenticators can be used to authenticate the connection and acquire a Passport.

- **Require a web login** — You can require an HTTP connection to acquire an Active Passport. Users are redirected from a web request to an authentication logon page, or they can go directly to the web logon page. Active Passport authentication for other connection types are denied.

After a user has been authenticated, a “Successful Login” browser window appears and the user is redirected to the requested web page. Any type of connection with an Active Passport authentication method is then allowed for the life of the Active Passport.

- **Active session mode** — You can use active session mode with web logon to require the Active Passport holder to maintain an open HTTP network connection to the firewall. This increases security when multiple users share the same IP address, for example, if a computer is shared or if users connect through a VPN concentrator.

When active session mode is enabled, the “Successful Login” browser window must remain open during the life of the Active Passport. Other browser windows must be used to access web sites. If the user was redirected to the web logon page, the “Successful Login” browser window contains a link to the requested web page.

A heartbeat message periodically tests the HTTPS connection and refreshes the “Successful Login” web page. If the connection is broken, the Active Passport is revoked. The Active Passport can also be revoked by clicking **Stop** on the browser window, closing the browser window, or restarting the computer. When an Active Passport is revoked, all of the sessions that were authorized by that Active Passport are closed.

- **Other authentications** — Because an Active Passport holder does not need to be authenticated for subsequent connections, Active Passport can be used for encrypted services or for services that do not have an authentication mechanism, such as ping.

Configure Active Passport

Configure the firewall to authenticate users with Active Passport.

Select **Policy > Rule Elements > Passport**.




Tip: For option descriptions, click **Help**.

Create and modify Active Passports using these tasks.

Configure an inband Active Passport

Configure Active Passport to authenticate inband.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) On the **General** tab, make the following selections:
 - **Inband**
 - **Authenticators used to establish Passport credentials** — Select the authenticators that can be used to acquire an Active Passport. Configured authenticators populate this list.
 - **Default authenticator** — Select the authenticator used by default for connections that have Passport as the authenticator on the **Rules Properties** window.
- 2) On the **Advanced** tab, configure the **Active authentication options**.
- 3) Save your changes.

Require an HTTP connection to acquire an Active Passport

Users will need to authenticate through a web page before they are assigned an Active Passport.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) On the **General** tab, make the following selections:
 - **Web login**
 - **Authenticators used to establish Passport credentials** — Select the authenticators that can be used to acquire an Active Passport. Configured authenticators populate this list.
 - **Default authenticator** — Select the authenticator used by default for access control rules that have **<None/Passport>** as the authenticator.
- 2) In the **Advanced** tab, configure the **Active authentication options** and **Web login** settings.
- 3) Save your changes.

Users can also access the authentication logon page by directing their browser to:

`https://firewall_address:8111/login.html`

If a user wants to log off of the Active Passport cache manually (before their authentication cache expires), they can point their browser to:

`https://firewall_address:8111/logout.html`

Require an Active Passport holder to maintain an open network connection to the firewall

Require a user to maintain an active connection through the firewall to keep their Active Passport.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) On the **General** tab, make the following selections:
 - **Web login with active session mode**
 - **Authenticators used to establish Passport credentials** — Select the authenticators that can be used to acquire an Active Passport. Configured authenticators populate this list.
 - **Default authenticator** — Select the authenticator used by default for access control rules that have **<None/Passport>** as the authenticator.
- 2) On the **Advanced** tab, configure the Active authentication options and Web logon settings.
 - Use the **Refresh period** field to configure how frequently a heartbeat message is sent to the “Successful Login” web page. A heartbeat message periodically tests the HTTPS connection and refreshes the page. If the connection is broken, the Active Passport is revoked.
 - Use the **Grace period** field to configure how many seconds the HTTPS connection can be broken before the Active Passport is revoked.



Note: Timeouts vary among web browsers. A high refresh period could result in revoked Active Passports for some browsers due to the HTTPS connection timing out.

- 3) Save your changes.

Revoke the Active Passport authentication cache for users

Revoking an Active Passport forces the user to authenticate to the firewall at the next connection.

Steps

- 1) Click **Manage Passports**.



Tip: For option descriptions, click **Help**.

- 2) Select a user and click **Revoke Passport(s)**.
To revoke all users, click **Revoke All Passports**.

- 3) Click **Close**.

Result



Note: This revokes only Active Passports.

Browser settings for non-transparent Active Passport

Users connecting over non-transparent HTTP or HTTPS must correctly configure their browser proxy settings to access the authentication page.

Specifically, users must:

- Create an exception for the firewall address on port 8111.
- Configure a separate port for secure connections.

Configure Passport for Internet Explorer

Configure browser settings for Microsoft Internet Explorer 8.

Steps

- 1) Select **Tools > Internet Options > Connections**.
- 2) Select the connection to configure and click **Settings** or **LAN settings**. The settings window appears.
- 3) Select the **Use a proxy server for this connection** checkbox, then click **Advanced**. The **Proxy Settings** window appears.
- 4) In the **HTTP** field, type the firewall address and port 80.
- 5) In the **Secure** field, type the firewall address and port 443.
- 6) [Conditional] If the clients are using non-transparent HTTP, in the **Exceptions** field, add an entry in the form `<firewall_address>:8111`.
Example: 192.0.2.0:8111



Tip: Alternatively, on the settings window, you can select the **Bypass proxy server for local addresses** checkbox.

- 7) Click **OK**, then click **OK** again.

Configure Passport for Firefox

Configure browser settings for Mozilla Firefox 3.6.

Steps

- 1) Select **Tools > Options > Network**.
- 2) Click **Settings**. The **Connection Settings** window appears.
- 3) Select the **Manual proxy configuration** option.
- 4) In the **HTTP Proxy** field, type the firewall address; in the **Port** field, type 80.

- 5) In the **SSL Proxy** field, type the firewall address; in the **Port** field, type 443.
- 6) [Conditional] If the clients are using non-transparent HTTP, in the **No Proxy for** field, add an entry in the form `<firewall_address>:8111`.
Example: 192.0.2.0:8111
- 7) Click **OK**, then click **OK** again.

Authenticator configuration

When users trying to make a network connection match an access control rule, you can use authenticators to validate their identity.

- 1) You configure an authenticator on the **Authenticators** window.
- 2) Select the authenticator in the access control rule.
- 3) A user matching the rule is prompted to provide a user name and valid password and/or a special passcode or personal identification number (PIN) before being logged on to a server.

Authenticators can be used to establish Active Passport credentials, which caches the source IP address so that subsequent connections are not prompted for authentication.

The following applications support authenticators:

- Admin Console
- HTTP and HTTP-based applications
- FTP
- Login Console
- SOCKS Proxy
- Telnet
- Telnet Server
- SSH Server

Authenticator options

You can create the following authenticators on the firewall.

- **Password** — Standard password authentication requires users to enter the same password each time they log on. The user database is maintained on the firewall.
Standard password authentication is typically used for internal-to-external SOCKS5, Telnet, FTP, and HTTP connections, and for administrators logging on to the firewall from the internal (trusted) network.
Password is a default authenticator. It cannot be deleted.
- **LDAP (Lightweight Directory Access Protocol)** — Four types of LDAP authentication are available: iPlanet, Active Directory, OpenLDAP, and Custom LDAP.
Use LDAP to provide fixed password authentication for SOCKS5, Telnet, FTP, and HTTP sessions through the firewall. It can also be used to authenticate logons and SSH logons to the firewall
- **CAC (Common Access Card)** — Use this authenticator to log on to a firewall using a U.S. Department of Defense Common Access Card.



Note: For complete instructions on configuring and using a CAC authenticator, see the application note about configuring Department of Defense Common Access Card authentication at <https://support.forcepoint.com>.

- **Windows domain** — You can use this authenticator if your organization operates a Windows primary domain controller (PDC) or backup domain controller (BDC).

Use a Windows primary domain controller (PDC) or backup domain controller (BDC) to provide password authentication for logon, SOCKS5, Telnet, FTP, HTTP, and SSH sessions to the firewall.



Note: Be sure the domain controller does not allow blank or default logons that can be easily guessed by outsiders.

For browsers that support it, you can also use transparent browser authentication (also known as NTLM or integrated Windows authentication). For more information about configuring your organization's PDC or BDC to use transparent browser authentication on the firewall, see the related application note located at <https://support.forcepoint.com>.

- **RADIUS** — You can use this authenticator if your organization operates a RADIUS server. RADIUS is a standard protocol used to authenticate users before they are allowed access to your system. Use RADIUS to provide authentication for SOCKS5, Telnet, FTP, and HTTP sessions through the firewall. RADIUS can also be used to authenticate logons and SSH logons to the firewall.

Manage authenticators

Create and manage authenticators.

Select **Policy > Rule Elements > Authenticators**.





Tip: For option descriptions, click **Help**.

You can perform the following tasks on the **Authenticators** window.

Table 27: Authenticator tasks

Task	Steps
Create a new authenticator	<p>To create LDAP, Windows domain, and RADIUS authenticators, see the following tasks:</p> <ul style="list-style-type: none"> • Configure an LDAP authenticator • Configure a Windows domain authenticator • Configure a RADIUS authenticator <p>Note the following:</p> <ul style="list-style-type: none"> • Password is a default authenticator that can be modified. You cannot create a new password authenticator. • To configure and use a CAC authenticator, see the application note about configuring Department of Defense Common Access Card authentication at https://support.forcepoint.com.

Task	Steps
Modify an authenticator	<ol style="list-style-type: none"> 1) Select an authenticator in the list. 2) Modify the settings in the lower pane, or click Modify and make your changes in a pop-up window. 3) Save your changes.
Delete an authenticator	<ol style="list-style-type: none"> 1) Select an authenticator in the list. 2) Click Delete. 3) Save your changes. <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Note: Password is a default authenticator and cannot be deleted. </div>
Rename an authenticator	<ol style="list-style-type: none"> 1) Select an authenticator in the list. 2) Click Rename. 3) Enter a new name in the pop-up window. 4) Click OK and save your changes. <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Note: Password is a default authenticator and cannot be renamed. </div>
View where an authenticator is being used	<ol style="list-style-type: none"> 1) Select an authenticator in the list. 2) Click Usage.
Block access after consecutive failed authentication attempts	<ol style="list-style-type: none"> 1) Click Manage Authentication Failures. 2) Select Enable. 3) In the Lockout Threshold field, enter the number of authentication attempts allowed before a user is locked out. 4) Click OK and save your changes.

Related tasks

- [Configure an LDAP authenticator](#) on page 103
- [Configure a Windows domain authenticator](#) on page 103
- [Configure a RADIUS authenticator](#) on page 104

Configure an LDAP authenticator

Configure the firewall to connect to an LDAP server to authenticate users.

Steps

- 1) Click **New**, then select one of the LDAP authenticators from the submenu:



Tip: For option descriptions, click **Help**.

- **iPlanet**
 - **Active Directory**
 - **Open LDAP**
 - **Custom LDAP**
- 2) Enter a name and optional description.
 - 3) Complete the **General** tab.
 - Click **New** to configure a new server. Click the up and down arrows to rank the servers in the list.
 - Make entries in the **Login options** section to specify how the firewall will connect to LDAP servers.
 - 4) Click the **Search** tab and define the search parameters for LDAP authentication.
 - Enter the LDAP identifiers. (Custom LDAP only; these default attributes cannot be modified in the other LDAP authenticators.)
 - Define the search filter options.
 - Select which containers will be searched.
 - 5) Click **Add** and save your changes.

Configure a Windows domain authenticator

Configure the firewall to connect to a Windows domain server to authenticate users.

Steps

- 1) Click **New** > **Windows**.



Tip: For option descriptions, click **Help**.

- 2) Enter a name and optional description.
- 3) Complete the **General** tab.
 - Click **New** to configure a new domain controller. Click the up and down arrows to rank the domain controllers in the list.
 - [Optional] Modify the logon and password prompts and the failed authentication message that users see.
 - Select prompted or transparent browser authentication.

- 4) Click **Add** and save your changes.

Configure a RADIUS authenticator

Configure the firewall to connect to a RADIUS server to authenticate users.

Steps

- 1) Click **New > RADIUS**.



Tip: For option descriptions, click **Help**.

- 2) Enter a name and optional description.
- 3) Complete the **General** tab.
 - Click **New** to configure a new server. Click the **up** and **down** arrows to rank the servers in the list.
 - [Optional] Modify the logon and password prompts and the failed authentication message that users see.
- 4) Click the **Groups** tab and enter the attributes defined in the dictionary files on the RADIUS server.
- 5) Click **Add** and save your changes.

User password management

Users can switch authentication methods or change their own passwords.

Switching authentication methods during a logon session

The firewall allows you to use multiple authentication methods for a given access control rule (for example, users might use RADIUS or Password for Telnet authentication). When logging on, a user can change to another authentication method by typing `:authenticator` after the user name.

Setting up users to change their own passwords

The Change Password Server allows users to use a web browser to change their firewall or LDAP logon password.

To allow this process, you must do the following:

- Create an access control rule that allows users to change their passwords.
- Inform users how they can change their own passwords using a web browser.

Create a change password rule

Create a rule for the Change Password Server.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Select the appropriate settings from the following table.



Tip: For option descriptions, click **Help**.

Table 28: Access control rule settings to allow users to change their logon passwords

Criteria	Setting
Action:	Allow
Application:	Change Password Server
Source Zone:	Desired zone (for example, internal)
Destination Zone:	Desired zone (for example, internal)
Source Endpoint:	Site dependent
Destination Endpoint:	localhost (a default host object)
Redirect:	<Firewall> (IP)
Redirect port:	1999

Change user passwords

With standard password authentication, users can change their passwords from a web browser.

Using standard password authentication, you can authenticate trusted and Internet users who request SOCKS5, FTP, HTTP, and Telnet access by way of proxies.

As an administrator, you should inform those users how they can change their own password from their terminal or computer by using a web browser.

However, there are some restrictions:

- Users can change their own password only if they are using standard password or LDAP authentication.
- To allow users to change their logon passwords, you must first create a rule for the firewall to allow this.

To change a user password:

Steps

- 1) Start a web browser.
- 2) [Conditional] If you are using a non-transparent proxy, configure your browser not to proxy requests going to the firewall on port 1999.

- 3) Open an HTTP connection to your firewall. For example: *http://myfirewall.example.com:1999/*
A pre-defined HTML change password form appears.
- 4) Enter your user name.
- 5) Enter your current password. This is your current password for establishing network connections.
- 6) Enter your new password. This will be your new password for establishing network connections.
- 7) Re-enter the new password. This confirms the spelling of the new password.
- 8) Select one of the following password types:
 - If you are changing a firewall logon password, select **Password**.
 - If you are changing an LDAP password, select **LDAP**.
- 9) Click **Send Request**.

Result

This sends the change password request to the firewall. You will be notified if the request failed or if it is accepted. If the request is accepted, the password database is updated and the new password must be used for all future connections.

Users and user groups

A user is a person who uses the networking services provided by the firewall. A user group is a logical grouping of one or more users, identified by a single name. Users and groups can be used to match access control rules and SSL rules.



Note: Users that do not match a rule are not explicitly denied and could be allowed by a subsequent rule.

You can configure the following types of users and user groups on Sidewinder:

- **Firewall user** — User and password information is configured and stored on the firewall.
 - Administrators are created on the **Administrator Accounts** window. They appear in user lists as a firewall user.
 - Administrators connect to the firewall. Other users connect through the firewall.
- **Firewall user group** — The group is configured and stored on the firewall. Members you add to the group can include any of the following:
 - Firewall users and user groups
 - External groups
 - Logon Collector users, groups, and distribution lists



Note: Both a firewall group and its individual group members appear in the **Users and User Groups** list. Firewall user group members are treated individually on access control rules and SSL rules, and they appear individually in audits.

- **External group** — An external group configured on the firewall corresponds to a group configured and stored on an LDAP or RADIUS authentication server. The group names are compared for a match in access control rules and SSL rules.
- **MLC user** — A Logon Collector user configured on the firewall is a placeholder for a corresponding user that has not yet been configured on an Active Directory server. When the user is added to the Active Directory server, you do not need to update access control rules or SSL rules this user is included in. Logon Collector also works in conjunction with McAfee EIA to collect user credentials.
- **MLC group** — A Logon Collector group configured on the firewall is a placeholder for a corresponding group that has not yet been configured on an Active Directory server. When the group is added to the Active Directory server, you do not need to update access control rules or SSL rules this group is included in.
- **MLC distribution list** — A Logon Collector distribution list configured on the firewall is a placeholder for a corresponding distribution list that has not yet been configured on an Active Directory server. When the distribution list is added to the Active Directory server, you do not need to update access control rules or SSL rules this distribution list is included in.

To configure users and user groups:

- 1) Select **Policy > Rule Elements > Authenticators**.
- 2) Click **Users and Groups**. The **User and User Groups** window appears.



Tip: For option descriptions, click **Help**.

You can perform the following tasks to manage users and user groups:

Related concepts

[How McAfee EIA works](#) on page 147

Related tasks

- [Create a firewall user](#) on page 108
- [Create a firewall user group](#) on page 108
- [Create an external group](#) on page 109
- [Create a McAfee Logon Collector user](#) on page 109
- [Create a McAfee Logon Collector group](#) on page 109
- [Create a McAfee Logon Collector distribution list](#) on page 110
- [Modify a firewall user or user group](#) on page 110
- [View where a user or group is being used](#) on page 111
- [Rename a user or group](#) on page 111
- [Delete a user or group](#) on page 111
- [Filter the list by type](#) on page 112
- [Search for a user or group in the list](#) on page 112

Create a firewall user

Create a new firewall user.

Steps

- 1) Click **New** > **Firewall user**.



Tip: For option descriptions, click **Help**.

- 2) Enter identifying information in the **User Information** tab.
- 3) Click the **User Password** tab and enter a password or generate a password automatically.
- 4) Click **OK** and save your changes.

Create a firewall user group

Create a group of users that have been configured on the firewall.

Steps

- 1) Click **New** > **Firewall user group**.



Tip: For option descriptions, click **Help**.

- 2) Enter a firewall group name and optional description.
- 3) On the **Groups** tab, select the **Member** checkbox next to the groups or distribution lists you want included in the firewall user group.
- 4) On the **Users** tab, select the **Member** checkbox next to the users you want included in the firewall user group.
- 5) Click **OK** and save your changes.

Result



Note: You can click **New** on either tab to create users or user groups.

Create an external group

Create a user group that corresponds to a group on your external authentication server.

Steps

- 1) Click **New > External group**.



Tip: For option descriptions, click **Help**.

- 2) Enter a name for the group. The name must exactly match the name on the external authentication server.
- 3) Click **OK**.

Create a McAfee Logon Collector user

Create a McAfee Logon Collector user.

Steps

- 1) Click **New > Firewall user group**.



Tip: For option descriptions, click **Help**.

- 2) Click the **Users** tab.
- 3) Click **New > MLC user**.
- 4) Enter the name of the user as it will be configured on the Active Directory server.
- 5) Click **OK**.

Create a McAfee Logon Collector group

Create a McAfee Logon Collector group.

Steps

- 1) Click **New > Firewall user group**.



Tip: For option descriptions, click **Help**.

- 2) On the **Groups** tab, click **New > MLC group**.
- 3) Enter the name of the group as it will be configured on the Active Directory server.

- 4) Click **OK**.

Create a McAfee Logon Collector distribution list

Create a placeholder for a distribution list that has not yet been configured on the Active Directory server.

Steps

- 1) Click **New > Firewall user group**.



Tip: For option descriptions, click **Help**.

- 2) On the **Groups** tab, click **New > MLC distribution list**.
- 3) Enter the name of the distribution list as it will be configured on the Active Directory server.
- 4) Click **OK**.

Modify a firewall user or user group

Modify users or user groups.

Steps

- 1) Select a user or group in the list, then click **Modify**.



Tip: For option descriptions, click **Help**.

- 2) Make your changes in the pop-up window.
- 3) Click **OK**.

Result



Note: You can modify only firewall users and user groups.

View where a user or group is being used

View the rules that reference a particular user or user group.

Steps

- 1) Select the user or group you want to investigate.



Tip: For option descriptions, click **Help**.

- 2) Click **Usage**.
The **Usage** window appears.

Rename a user or group

Rename users or user groups.

Steps

- 1) Select the user or group you want to rename.



Tip: For option descriptions, click **Help**.

- 2) Click **Rename**.
- 3) Enter a new name.
- 4) Click **OK**.

Delete a user or group

Delete users or user groups.

Steps

- 1) Select the user or group that you want to delete.



Tip: For option descriptions, click **Help**.

- 2) Click **Delete**. A confirmation message appears.
- 3) Click **Yes**, then save your changes.

Result



Note: If you delete an administrator, that administrator will also be deleted from the **Administrator Accounts** window. If you delete an administrator from the **Administrator Accounts** window, that administrator will also be deleted from the **Users and User Groups** window.

Filter the list by type

Filter the list of users and user groups that are shown

In the **Show** area, select one or more user and group options.

To clear a category filter, deselect the category.

Search for a user or group in the list

Filter the list of users or groups displayed.

In the **Search** field, type your search criteria. Items are filtered based on the characters entered.



Tip: To reset your search, click the **X** in the **Search** field.

Content inspection

Contents

- [Methods of content inspection](#) on page 113
- [Configure IPS inspection](#) on page 114
- [Configuring virus scanning](#) on page 125
- [How McAfee Global Threat Intelligence works](#) on page 128
- [Benefits of SmartFilter](#) on page 136

Sidewinder content inspection methods provide additional security features by examining the content of a connection after it has matched an access control rule.

Methods of content inspection

The following methods are available for content inspection.

- **Intrusion Prevention System (IPS)** — IPS is a signature-based inspection tool that identifies attacks before they pass through the Sidewinder.
- **Virus scanning** — The anti-virus service is a licensed add-on module that uses a firewall-hosted virus scanner that allows you to configure rule-based MIME, virus, and spyware scanning.
- **Global Threat Intelligence** — Global Threat Intelligence is an Internet reputation service that assigns a reputation score to an IP address based on the behavior attributes of the traffic it generates. A reputation score is like a credit score that indicates the trustworthiness of an IP address.
- **SmartFilter** — SmartFilter is a content management solution that controls your company's users' access to the Internet.

Once a content inspection method is configured, it becomes available for selection on access control rules or in some cases Application Defenses.

Related concepts

- [Configuring virus scanning](#) on page 125
- [How McAfee Global Threat Intelligence works](#) on page 128
- [Benefits of SmartFilter](#) on page 136

Related tasks

- [Configure IPS inspection](#) on page 114

Configure IPS inspection

The Sidewinder Intrusion Prevention System (IPS) is a signature-based inspection tool that identifies attacks before they pass through the firewall.

IPS plays an important role in protecting hosts and services that have known vulnerabilities and exploits, yet are required components of your organization.



Note: For IPS conceptual information, review *How IPS inspection works*.

To configure IPS inspection:

Related concepts

[Configuring a response mapping](#) on page 118

[Configuring a signature group](#) on page 120

[Managing signatures](#) on page 123

[Adding IPS inspection to access control rules](#) on page 124

How IPS inspection works

The Sidewinder IPS inspection uses signatures to detect and prevent known network-based intrusion attacks, such as hacker-generated exploits.

How the firewall responds to an attack is configurable; options range from allowing but auditing the attack to blackholing all traffic coming from the attacker.

IPS inspection is enforced on access control rules. Each access control rule that uses IPS inspection is assigned a *signature group* and a *response mapping*. The signature group is used to limit scanning to relevant signatures. The response mapping specifies the action to take when a packet or session is identified as an attack.

IPS signatures

The foundation of IPS inspection is its *signatures*. The signatures are the data for recognizing attacks. Each signature has a *category* attribute, a *threat level* attribute, and a *class type* attribute.

The signature category is classified by the network service targeted for attack, and consists of a main category and a subcategory. The class type identifies the attack's intended purpose, such as *Root Level Exploit* or *Discovery*. One or more categories can be added to a signature group. For example, to create a signature group for an inbound Oracle server access control rule, create a group named Oracle that includes the categories DB:Oracle, Component:Encoder, and Component:Shellcode. The firewall also provides default signature groups based on common attack targets, such as the Database Servers group and the Internal Desktops group.

Within each category and response mapping, the signatures have a threat level attribute: IPS or IDS. This threat level indicates a relationship between confidence level and severity. Signatures classified as IPS detect attacks that are considered dangerous. Signatures classified as IDS detect attacks that are either considered minor, such as probe or discovery activity, or they are suspected attacks, meaning the signature might be likely to incorrectly identify legitimate traffic as an attack. The default signature groups and response mappings include both the IPS and IDS threat levels.

Signatures classified as *Policy* identify network traffic that you want to control based on your organization's security policy, such as instant messaging or P2P communication. Policy signatures are added individually

to a signature group—they are not included in the default signature categories since they are specific to an organization.

IPS responses

Based on class type and threat level, you configure the response the firewall will take when an attack matches a signature.

Options are:

- **Allow no audit** — Allows the traffic to pass and does not generate an IPS audit event. This is the default for all class types when creating a new response mapping.
- **Allow** — Allows the traffic to pass and generates an IPS audit event. Use this setting for traffic that is an anomaly and appears suspicious but is not an identifiable attack.
- **Drop** — Denies only those packets that are suspect while allowing trusted packets. The firewall will not alert the attacker that the connection was closed. This generates an IPS audit event.
- **Deny** — Similar to **Drop** except that this response sends a TCP reset informing the originating host the connection was deliberately closed. This generates an IPS audit event.



Note: Use this setting only when troubleshooting or when instructed by technical support. Sending a TCP reset or other connection-denied response could notify the attacker that the firewall has recognized the attack, prompting the attacker to switch to a new attack.

- **Deny no audit** — Similar to **Deny** except that this response does not generate an IPS audit event.
- **Blackhole** — Denies all traffic from the host originating the hostile traffic for a set period of time. This generates an IPS audit event. The firewall will not alert the attacker that the connection was closed. Use this setting when you are sure all traffic coming from an address is malicious.

In general, the response should correspond to the severity of the attack. Categories labeled IDS might generate some false positives or might be probing or discovery attacks. Therefore, attacks of this threat level should generally never be blackholed.

For example, to create a response mapping that protects against root level exploits against an Oracle server, create a mapping named Oracle and set Root Level Exploit type IDS to Allow and Root Level Exploit type IPS to Blackhole for 10,000 seconds.

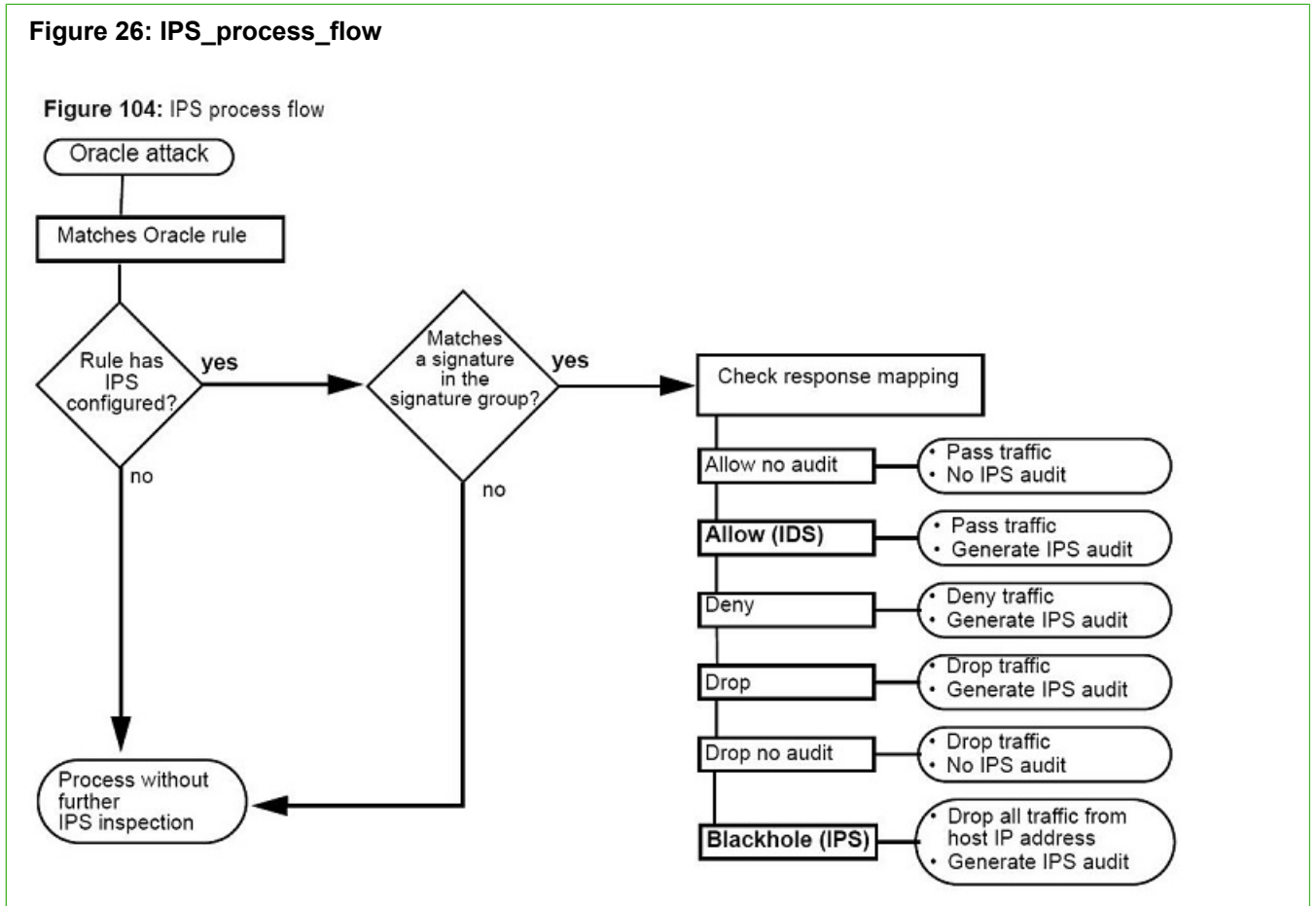
IPS processing example

IPS processing is performed in a particular order.

In this example:

- 1) An Oracle attack matches an Oracle access control rule.
- 2) IPS inspection is enabled on the Oracle access control rule.
- 3) The packet is compared to the signatures in the signature group and a match is found.
- 4) The firewall checks the access control rule's response mapping for instructions on responding to the attack.
 - If the identified attack matches a signature with a threat level of IDS, the connection is allowed through but generates an IPS audit event.
 - If the identified attack matches a signature with a threat level of IPS, the connection is blackholed for 10,000 seconds, so all traffic from the source's IP address is blackholed for that length of time.

Figure 26: IPS_process_flow



Using IPS with other Sidewinder attack protection tools

Sidewinder supports several different scanning tools to help detect harmful connections.

There are several different approaches to protecting your internal network. One approach is to prohibit any traffic from entering your network. While this solution is secure, it is also impractical. Another approach is to attempt to scan all incoming traffic for known attacks, viruses, etc., but this can slow down the firewall, and therefore your network connectivity.

The best solution is first use tools to minimize your network’s attack surface, and then use scanning to protect services that must be allowed. You can reduce your network’s attack surface by creating the minimum number of access control rules necessary to allow essential inbound traffic and limiting the source and destination endpoints to hosts or address ranges. In addition, Application Defenses can be used to further refine what traffic is allowed into your network by prohibiting unnecessary commands, header, protocol versions, and other parameters. Once your policy is sufficiently restrictive, use IPS and other signature-based services such as anti-virus to inspect traffic destined for vulnerable yet essential services.

For example, an administrator is running a web server that requires allowing inbound HTTP traffic. The administrator knows that the Content Length header and the Content Location header are often used in attacks. The Content Location header is not required by the web server, and therefore does not need to be allowed into the network. The administrator uses the HTTP Application Defense to deny that header. The Content Length header is required, so the administrator allows it but adds IPS inspection to the access control rule allowing that traffic to make sure known attacks using that header are blocked.

While a small attack surface and inspection tools are a strong defense, you should still use Attack Responses to monitor attack activity. Even attacks that are not allowed through the firewall are noteworthy as they might be an attempt from a hacker who will later try a more sophisticated attack. Attack Responses can send out alerts when your network is under attack. These alerts will notify you of situations that might require a configuration change to increase the security of your network or investigation into the reason for the attack.

Related concepts

[Managing attack responses](#) on page 318

Verify that your firewall is licensed for IPS

To enable IPS inspection, the IPS and IPS Signature features must be licensed.

To verify that these features are licensed:

Steps

- 1) Select **Maintenance > License**, then click the **Firewall** tab.



Tip: For option descriptions, click **Help**.

- 2) If you are not licensed for IPS and IPS Signature, contact your sales representative.

Download IPS signatures and enable automatic signature updates

Since new attacks are constantly identified, it is important to update the signatures frequently. When new signatures are added to the firewall, they go into effect based on how the existing signature categories and response mappings are configured.



Note: Policy signatures are not included by default in any signature category group and general class types are not applied to them. Therefore, new policy signatures must be specifically added to category groups in order to use them.

To download IPS signatures and configure automatic signature updates:

Steps

- 1) Select **Maintenance > Updates**.
- 2) In the upper pane, select **IPS signatures**.



Tip: For option descriptions, click **Help**.

- 3) Download the IPS signatures.
 - a) Click **Update Database Now**. A pop-up window appears.

- b) Click **Background** or **Wait**. The firewall downloads the IPS signatures.
- 4) Select **Enable automated updates**, then specify the update frequency.



Note: We recommend enabling automatic IPS signature updates.

- 5) Save your changes.

Related tasks

[Manage service updates](#) on page 600

Configuring a response mapping

A response mapping contains a list of class types, their threat level, and their response settings.

Each class type refers to a set of known network-based attacks. Class types classified as IPS detect confirmed attacks that are also considered dangerous. Class types classified as IDS detect either suspected attacks or traffic that is considered less dangerous, such as probe or discovery activity. Class types classified as Policy identify traffic based on organizational security practices.

Response mappings are configured on the **Response Mapping** tab. They can then be selected on the access control rule to determine how the firewall responds when an attack is detected.

To configure a response mapping, select **Policy > IPS**. The **Response Mappings** tab appears.

The upper pane contains the toolbar and the existing response mappings. When you select a mapping, its properties appear in the lower pane.

Use the toolbar and table in the upper pane to perform the actions listed here:

Table 29: Response Mappings toolbar

Button Menu item	Action
New	Create a new response mapping by clicking New . The New Response Mapping window appears.
Modify	Modify a response mapping: <ul style="list-style-type: none"> • Select it and modify its properties in the lower pane. • Double-click it and modify it in the new window. • Select it, click Modify, and edit it in the new window. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Note: Read-only administrators are not supported in 8.2.0. </div>
Delete	Delete a response mapping by selecting it and clicking Delete .
Duplicate	Create a copy of an existing response mapping by selecting the mapping, clicking Duplicate , and customizing the copy as needed.

Button Menu item	Action
Rename	Rename a response mapping by selecting it and clicking Rename .
Usage	View what access control rules currently use a response mapping by selecting a mapping and clicking Usage .
Find	Search for a specific element(s) in the list using the Find field. Type your search criteria, and response mappings with matching elements will appear in the list. Clear this field to see the full list again.

Create or modify response mappings

Create or modify IPS response mappings.

When you click **New**, **Modify**, or **Duplicate**, the **New/Modify Response Mapping** window appears.

Steps

- 1) In the **Name** field, enter a name that identifies the purpose of the response mapping.



Tip: For option descriptions, click **Help**.

For example, if you create two mappings to address different threat levels to your web servers, you would name them *web server high* and *web server low*.

Valid values include alphanumeric characters, dashes (-), underscores (_), and spaces (). However, the first and last character of the name must be alphanumeric. The name cannot exceed 100 characters. You can rename the mapping later.

- 2) [Optional] In the **Description** field, enter any useful information about this mapping. For example, a mapping that allows but audits probe and discovery attacks would have the description `Probe-Discovery audit only`.
- 3) In the **Class Types** area, identify the class types to which you want the firewall to respond by setting the responses to one of the following:



Note: Signatures with any risk of false positive are always given a threat level of IDS. Therefore, do not deny, drop, or blackhole traffic for class types with a threat level of IDS.

- **Allow no audit** — Allows the traffic to pass and does not generate an IPS audit event. This is the default for all class types when creating a new response mapping.
- **Allow** — Allows the traffic to pass and generates an IPS audit event. Use this setting for traffic that is an anomaly and appears suspicious but is not an identifiable attack.
- **Drop** — Denies only those packets that are suspect while allowing trusted packets. The firewall will not alert the attacker that the connection was closed. This generates an IPS audit event.
- **Deny** — Similar to Drop except that this response sends a TCP reset informing the originating host the connection was deliberately closed. This generates an IPS audit event.



CAUTION: Use this setting only when troubleshooting or when instructed by technical support. Sending a TCP reset or other connection-denied response could notify the

attacker that the firewall has recognized the attack, prompting the attacker to switch to a new attack.

- **Deny no audit** — Similar to Deny except that this response does not generate an IPS audit event.
- **Blackhole** — Denies all traffic from the host originating the hostile traffic for a set period of time. This generates an IPS audit event. The firewall will not alert the attacker that the connection was closed. Use this setting when you are sure all traffic coming from an address is malicious. In the **Duration** field, enter the time in seconds that the traffic will be denied.
 - Valid values are 0 and 1–100000 seconds.
 - To blackhole the host indefinitely, enter **0**. The host remains blackholed until it is deleted from the blackhole list in the dashboard or the firewall is restarted.



Tip: See the Dashboard to manage the blackholed IP addresses.

- 4) Click **Add**.
- 5) Save your changes.

Result

This response mapping is available for use in a access control rule.

Configuring a signature group

A signature group can contain one or more signature categories. A signature category is a category of signatures that all involve the same type of attack.

The IPS engine provides the categories and might update them occasionally.

You can also add individual signatures to a signature group. This gives you finer control in creating a signature group, and it allows you to add Policy signatures, which are not included in the default signature categories since they are specific to an organization.

Signature groups are configured on the **Signature Groups** tab. They can then be selected on access control rules to focus IPS inspection on relevant attacks.

To configure a signature group, select **Policy > IPS** and click **Signature Groups**. The **Signature Groups** tab appears.

The upper pane contains the toolbar and the existing signature groups. When you select a signature group in the list, the properties of that group appear in the lower pane.




Note: Policy signatures must be added to a signature group by using the **Select Additional Signatures** button.

Use the toolbar and table in the upper pane to perform the actions listed here:

Table 30: Signature Groups toolbar

Button/ Menu item	Action
New	Create a new signature group by clicking New . The New Signature Group window appears.

Button/ Menu item	Action
Modify	<p>Modify a signature group:</p> <ul style="list-style-type: none"> • Select it and modify its properties in the lower pane. • Double-click it and modify it in the pop-up window. • Select it, click Modify, and edit it in the pop-up window. <p> Note: Read-only administrators are not supported in 8.2.0.</p>
Delete	Delete a signature group by selecting it and clicking Delete .
Duplicate	Create a copy of an existing signature group by selecting the group, clicking Duplicate , and customizing the copy as needed.
Rename	Rename a signature group by selecting it and clicking Rename .
Usage	View what access control rules use a given signature group by selecting a group and clicking Usage .
Find	Search for a specific element(s) in the list using the Find field. Type your search criteria, and signature groups with matching elements will appear in the list. Clear this field to see the full list again.

Create or modify signature groups

Create or modify IPS signature groups.

When you click **New**, **Modify**, or **Duplicate**, the **New/Modify Signature Group** window appears.

Steps

- 1) In the **Name** field, enter a name that describes the purpose of the signature group.



Tip: For option descriptions, click **Help**.

For example, if you wanted a signature category that searches both HTTP and FTP attack signature files, you would name it `HTTP_FTP`.

Valid values include alphanumeric characters, dashes (-), underscores (_), and spaces (). However, the first and last character of the name must be alphanumeric. The name cannot exceed 256 characters. You can rename the mapping later.

- 2) [Optional] In the **Description** field, enter any useful information about this group.
For example, a signature category designed to inspect Oracle-related connections would be named `Oracle` and include the categories `DB:Oracle`, `Component:Encoder`, and `Component:Shellcode`
- 3) Configure the **Categories** area:
 - a) In the **Use** column, select each category to include in the signature group.

- b) For each selected category, select IPS, IDS, or both:
 - Select **IPS** to identify attacks that are an exact match to a signature file.
 - Select **IDS** to identify attacks that are considered minor, such as probe or discovery activity, or suspected attacks, meaning the signature might have incorrectly identified legitimate traffic as an attack.

Both options are selected by default.

- 4) [Optional] Click **Select Additional Signatures** to open a pop-up window and enable individual signatures to add to the signature group. The added signatures appear in the read-only **Signatures** field.
- 5) Click **Add** and save your changes.

Result

This signature group is now available for use in a access control rule.

Adding individual signatures to a signature group

Adding signatures individually gives you finer control in creating a signature group, and it also allows you to add Policy signatures, which are not included in the default signature categories since they are specific to an organization.

When you click **Select Additional Signatures**, the **Select Additional Signatures** window appears.

Use this window to add individual signatures to a signature group.


Related tasks

[Filter the table](#) on page 123

[View signature vulnerabilities](#) on page 123

Enable and disable signatures

A blue check mark in the **Enabled** column indicates that the signature is implicitly included in a category used by the signature group. These signatures cannot be disabled.

-  **Note:** To disable an implicit signature, use the **Signature Browser** tab. This disables the signature globally so it is not used by any access control rule to scan traffic.
- A green check mark in the **Enabled** column indicates that the signature has been added to the signature group. These signatures can be disabled.

To change the status of a signature:

Steps

- 1) Select a signature in the table and click **Enable** or **Disable**.



Tip: For option descriptions, click **Help**.

- You can select multiple signatures by pressing and holding the **Ctrl** key while selecting the appropriate signatures.
 - You can select a range of signatures by selecting the first signature in the range, pressing and holding the **Shift** key, and then selecting the last signature in the range.
- 2) Click **OK**. You return to the **Signature Groups** tab and the enabled signatures appear in the read-only **Signatures** field.

Managing signatures

Use the **Signature Browser** tab to view and manage available signatures.

You can:

- Filter signatures for easier viewing.
- Enable or disable signatures globally.
- View signature vulnerabilities on the Common Vulnerabilities and Exposures (CVE) website.

To manage signatures, select **Policy > IPS** and click the **Signature Browser** tab. The **Signature Browser** tab appears.

You can perform the following tasks.

Filter the table

The table lists available signatures on the firewall, along with information such as category, class type, and type. You can control what appears in the table for easier viewing and faster table loading.

- To view signatures of specific categories, click **Filter Categories**. In the pop-up window, select the signature categories that you want to view.
- To search for a specific element(s) in the table, type your search criteria in the **Find** field and then click **Find Now**. Signatures with matching elements will appear in the table. Clear this field and click **Find Now** to see the full table again.



Note: Disabled signatures and user-added signatures (enabled with a green check mark) appear no matter what is in the **Find** field.

Related tasks

[Filter categories](#) on page 124

View signature vulnerabilities

The Vulnerability column of the table lists a number assigned by Common Vulnerabilities and Exposures (CVE).

Two types of identifiers can appear for a signature:

- If **CVE** precedes the number, the vulnerability has been reviewed and accepted by CVE and is an official entry in the CVE list.
- If **CAN** or nothing precedes the number, the vulnerability is under review by CVE and is not yet an official entry in the CVE list.

Select a signature and click **View Vulnerabilities** to open a CVE web page with detailed information about the vulnerability for that signature.



Note: The **View Vulnerability** button is disabled if no identifier exists for the selected signature or if multiple signatures are selected.

Enable and disable signatures globally

By default, all signatures are available and can be used by an access control rule to scan traffic. An available signature is indicated by a green check mark in the **Enabled** column.

If a signature is disabled, the **Enabled** check box is cleared and the signature is not be used when scanning traffic, even if it is part of a signature group referenced in an access control rule. Disabling might help avoid false positives based on signature, for example, if a certain signature is identifying legitimate traffic as an attack.

To change the status of a signature, select a signature in the table and click **Enable** or **Disable**.

- You can select multiple signatures by pressing and holding the **Ctrl** key while selecting the appropriate signatures.
- You can select a range of signatures by selecting the first signature in the range, pressing and holding the **Shift** key, and then selecting the last signature in the range.

Filter categories

Use the **Category Filter** window to populate the **Signature Browser** tab with signatures of selected categories.

When you click **Filter Categories**, the **Category Filter** window appears.

- Select and clear categories individually by clicking the check box in the **View** column, or use the **Select All** and **Deselect All** buttons.
- Search for a specific element(s) in the list using the **Find** field. Type your search criteria, and signature categories with matching elements will appear in the list. The buttons become **Selected Filtered** and **Deselect Filtered**.
Clear this field to see the full list again.
- Select the **Remember this filter selection** check box to retain the selected categories. The next time you open an **IPS Signature Browser**, the same category filter will be used.

When you are done selecting the categories of signatures you want to view, click **OK**. Only signatures of the selected categories appear in the **Signature Browser**.

Adding IPS inspection to access control rules

IPS inspection is enforced on access control rules. Inspecting all traffic using IPS signatures can greatly reduce your firewall's performance.

Enabling IPS inspection only when needed allows you to focus your firewall's resources on traffic that is most likely to contain attacks, such as HTTP traffic. Use signature groups, which limit scanning to relevant areas of the signature file database, to improve inspection efficiency.

When planning your security policy, determine what traffic and systems are likely to be targets for network-based attacks. IPS is most commonly used to inspect inbound connections, since attacks typically come from external, untrusted sources. If an internal server, such as a web server on your DMZ, were to be compromised, scanning its outbound connections is useful for containing damage and preventing attacks from spreading to other systems. Enable IPS on the access control rules that govern likely targets. Traffic that does not have IPS inspection enabled will not be inspected for network-based attacks.



Tip: If you want to blackhole an attack that is identified by the signature-based IPS when it first occurs, set that action in the response mapping. If you want to blackhole an attack only if it occurs multiple times, set that action in the Attack Responses (**Monitor > Attack Responses**).

The following figure is an example of an access control rule with IPS inspection enabled. When HTTP traffic destined for the vulnerable `_web_server` reaches the firewall, the firewall checks that traffic against signatures in the "Web Server Attacks" signature group. When the traffic's pattern matches an attack, the firewall checks the "Exploit Protection" response mapping to see how it should respond to the associated class type for that attack.

Figure 27: IPS on an access control rule



- 1) Searches signatures related to web server attacks.
- 2) Checks this response mapping to see what it should do with the connection.

Related concepts

[Configuring access control rules](#) on page 197

Configuring virus scanning

You can configure virus scanning for the following applications.

- HTTP-based applications
- HTTPS-based applications (if decrypted by an SSL rule)
- FTP
- Sendmail

Configure virus scanning using the following procedures.

Related tasks

[Configure global virus scanning properties](#) on page 125

[Configure virus scanning signature updates](#) on page 127

[Enable virus scanning on an access control rule](#) on page 127

Configure global virus scanning properties

To configure global virus scanning properties, select **Policy > Application Defenses > Virus Scanning**.

The **Virus Scanning** window appears.



Tip: For option descriptions, click **Help**.

You can perform the following tasks on this window:

Configure the number of scanners

You can specify the number of scanner processes dedicated to various data sizes, allowing the firewall to process data more efficiently.

The **Scanners** column displays the number of configured scanner processes.



Tip: While using additional scanners can speed up virus scanning, it might slow down your firewall's overall performance. To make virus scanning more efficient, try using more restrictive MIME/Virus/Spyware rules in the appropriate Application Defenses.

To modify the number of scanner processes:

Steps

- 1) Selected **Unlimited**, then click **Modify**. The **Advanced: Edit Scanners** window appears.



Tip: For option descriptions, click **Help**.

- 2) Specify the number of scanners for this file size range.
 - Valid values are 1–10.
 - Scanner processes consume significant system resources. Increasing the total number of processes might negatively affect overall firewall performance. If you add additional scanner processes, monitor system performance to ensure that resources are being used efficiently and performance is not degraded.
- 3) Click **OK**.
- 4) Save your changes.

Modify general scanning properties

You can perform the following tasks in the lower half of the **Virus Scanning** window.

Table 31: Virus scanning properties tasks

Task	Steps
Modify scan buffer sizes	<ol style="list-style-type: none"> 1) Specify a new value in the Scan Buffer Size (KB) field or Archive Scan Buffer Size (MB) field as appropriate. 2) Save your changes.

Task	Steps
Modify the maximum number of files to scan in an archive	<ol style="list-style-type: none"> 1) Specify a new value in the Maximum Number of Files to Scan in an Archive field. 2) Save your changes.
Enable or disable scanning for password-protected files	<ol style="list-style-type: none"> 1) Select or clear the Scan Encrypted Files option. 2) Save your changes.

Configure virus scanning signature updates

To ensure that the anti-virus signatures used by the virus scanner are up to date, the firewall periodically downloads updates.

To configure signature updates, select **Maintenance > Updates**

Related tasks

[Manage service updates](#) on page 600

Enable virus scanning on an access control rule

To use virus scanning, you must enable it on an access control rule.

Steps

- 1) Configure virus scanning on the appropriate Application Defense profile:
 - a) Select **Policy > Application Defenses > Defenses**, then select the appropriate Application Defense type:



Tip: For option descriptions, click **Help**.

- **HTTP** — Applies to HTTP-based applications and HTTPS-based applications if decrypted by an SSL rule
 - **FTP** — Applies to FTP-based applications
 - **Mail (Sendmail)** — Applies to the Sendmail Sever application
- b) Select an existing Application Defense profile or create a new one.
 - c) In the **Enforcements** tab, select **MIME/Virus/Spyware**.
 - d) Click the **MIME/Virus/Spyware** tab, then configure it as appropriate.

- e) Save your changes.
- 2) Create an Application Defense group that contains the profiles you created.
 - a) Select **Policy > Application Defenses > Groups**.
 - b) Select an existing group or create a new one.
 - c) In the list of Application Defenses, select the profiles that you configured virus scanning for.
 - d) Save your changes.
 - 3) Modify the appropriate access control rule.
 - a) Select **Policy > Access Control Rules**.
 - b) Open the access control rule you want to enable virus scanning for, or create a new access control rule.
 - c) From the **Application Defense** drop-down list, select the Application Defense group you created in step 2.
 - d) Close the access control rule, then save your changes.

Result

Virus scanning is enabled on the access control rule.

Related concepts

[Managing Application Defense profiles](#) on page 191

How McAfee Global Threat Intelligence works

Global Threat Intelligence is an Internet reputation service that assigns a reputation score to an IP address based on the behavior attributes of the traffic it generates.

A reputation score is like a credit score that indicates the trustworthiness of an IP address.

Global Threat Intelligence servers around the world gather and analyze billions of packets dynamically to determine reputation scores. For each IP address on the Internet, Global Threat Intelligence calculates a reputation value based on such attributes as sending behavior, blacklist and whitelist information, and spam trap information.



Note: Global Threat Intelligence does not support IPv6.

Reputation is expressed in four classes:

- **Minimal Risk (Low Risk)** — Our analysis indicates this is a legitimate source or destination of content/traffic.

- **Unverified** — Our analysis indicates that this appears to be a legitimate source or destination of content/traffic, but also displays certain properties suggesting that further inspection is necessary.
- **Medium Risk** — Our analysis indicates that this source/destination shows behavior we believe is suspicious and content/traffic to or from it requires special scrutiny.
- **High Risk** — Our analysis indicates that this source/destination does or will send/host potentially malicious content/traffic and we believe it presents a serious risk.



Note: See the Global Threat Intelligence website at <http://www.mcafee.com/us/threat-center.aspx> to check the reputation of your domain or specific IP addresses.

Using Global Threat Intelligence on your firewall can:

- Block spam email from botnets.
- Help prevent hosts on your network from being infected with botnet agents.
- Identify hosts on your network that have been compromised in botnet or pharming attacks.
- Protect critical servers from being inadvertently accessed by authorized users using external computers that are compromised.

Today's advanced malware attacks can utilize multiple network protocols to not only compromise a network but also to provide channels of communication back to the attacker. These communications can be used for further instructions or to send data back. For example, a common blended attack uses a phishing email to get a user to click on a link to a web site, which then installs malware on the user's computer over FTP. Global Threat Intelligence can determine the reputation of connection IP addresses and enforce policy accordingly.

Deployment considerations

These topics address common Global Threat Intelligence deployment questions.

Minimal latency

We minimize latency in these ways:

When a connection requires a Global Threat Intelligence reputation lookup, some latency is inevitable.

We check reputation only when it is required to decide how to handle a connection. If the security policy allows a decision without a reputation check, none is made. In normal network usage patterns, the intelligent caching architecture resolves most connections without a live reputation query.

There are several Global Threat Intelligence data centers located around the world. When a query is made, your firewall automatically directs it to the server that can give you the fastest response, usually in under 100 milliseconds. The result is little to no latency added for most applications.

Low firewall CPU consumption

In worst-case system tests, reputation queries never consumed more than two percent of the system CPU.

Configurable Global Threat Intelligence default reputation

If your firewall cannot reach any of the Global Threat Intelligence servers, it automatically assigns a default reputation to all applicable connections. The default reputation is configurable in the Admin Console.

The firewall checks periodically for server availability. As a result, users don't suffer any latency waiting for reputation queries to time out, and you control how traffic is handled in this situation.

Large amounts of traffic validation and latency monitoring

Reputation values are cached, and query responses are processed out of order to avoid bottlenecks.

The policy subsystem on the firewall monitors latency in Global Threat Intelligence queries. If there are delays for any reason, the firewall proactively reverts to using the default reputation until a reliable connection can be made.

Reputation query security

All queries from your firewall to the Global Threat Intelligence data centers occur through an encrypted tunnel that is secured with bidirectional certificate authentication. If the firewall detects a man-in-the-middle attack, it alerts you and reverts to using default reputation.

Enabling Global Threat Intelligence and information privacy

A reputation query implicitly tells the reputation server that a connection was attempted. This data is statistically mingled with other queries, and providing key input to the behavioral analysis algorithms that produce Global Threat Intelligence reputations. The reputation database is too large and dynamic to practically distribute to individual systems. While the firewall does not inspect this data, it does take measures to protect it. If the traffic patterns passing through your firewall are themselves highly confidential, avoid using reputation in your policy.

Using Global Threat Intelligence in access control rules

Global Threat Intelligence can be enabled on any access control rule that uses a TCP- or UDP-based application.

Traffic is not explicitly allowed or denied based on a Global Threat Intelligence reputation score. The score is one of the elements in the access control rule that is examined for a match.

When an access control rule examines a packet, the firewall queries a Global Threat Intelligence server to get the reputation score of all IP addresses involved in the connection.

- Private IP addresses are not evaluated by Global Threat Intelligence or examined in access control rules (for example, 10.x.x.x, 172.16.x.x, 192.168.x.x).
- Global Threat Intelligence queries are cached; if the firewall recently examined an IP address, there is no additional query to the Global Threat Intelligence server.
- Whitelist network objects to exempt them from Global Threat Intelligence requirements. This is useful for routable internal addresses or trusted external sources. Configure the whitelist on the GTI Reputation window.

Related concepts

[Configure Global Threat Intelligence settings](#) on page 133

Configuring an allow access control rule

You can configure an allow access control rule to match the following Global Threat Intelligence host reputation classes.

- **Low**
- **Unverified and below**
- **Medium and below**
- **None**

Global Threat Intelligence matches as follows:

- If the reputation score is within the selected reputation class(es) and all other elements in the access control rule match, the connection is allowed. No other access control rules are queried.
- If the reputation score is *not* within the selected reputation class(es), it is not a match. The connection is passed to the next access control rule.

Configuring a deny access control rule

You can configure a *deny* or *drop* access control rule to match the following Global Threat Intelligence host reputation classes.

- **None**
- **High**
- **Medium and above**
- **Unverified and above**

Global Threat Intelligence matches as follows:

- If the reputation score is within selected reputation class(es) and all other elements in the access control rule match, the connection is denied or dropped. No other access control rules are queried.
- If the reputation score is *not* within the selected reputation class(es), it is not a match. The connection is passed to the next access control rule.

Global Threat Intelligence access control rule example

You can use multiple Global Threat Intelligence access control rules together to selectively block or allow traffic.

For example, you might want to block inbound mail from High risk sources and accept mail from other sources. To do so, create two SMTP application access control rules that use Global Threat Intelligence as shown in the following table.

Table 32: Inbound SMTP access control rules using Global Threat Intelligence

Rule position	Rule action	Application	Selected reputation classes
n	Deny or Drop	SMTP	High
$n+1$	Allow	SMTP	Medium and below

Using Global Threat Intelligence with Geo-Location

You can restrict connections from a country to include only those that have a positive web reputation.

Assume you want to allow contractors and business contacts in Nigeria to connect with your network, but you want to restrict connections from IP addresses with a medium- or high-risk rating. Traffic that does not match the additional parameters of country and rating will be passed to the next access control rule.

Use this type of policy to protect your network from inbound potential malware.

Implementing this scenario involves these high level tasks:

- 1) Create an allow access control rule with a Geo-Location Source Endpoint of Nigeria.
- 2) Select the Global Threat Intelligence host reputation of **Unverified and below**.
- 3) Configure users and destination endpoints as needed.

- 4) Order your rule as needed.

Using Global Threat Intelligence with sendmail

If you use sendmail, you can use Global Threat Intelligence to filter incoming email connections by allowing messages only from senders with a reputation score below a defined threshold.

Before you enable Global Threat Intelligence filtering for sendmail, make sure your firewall is:

- Running sendmail
- Located at the perimeter of your network
- Able to access the Internet and resolve DNS queries

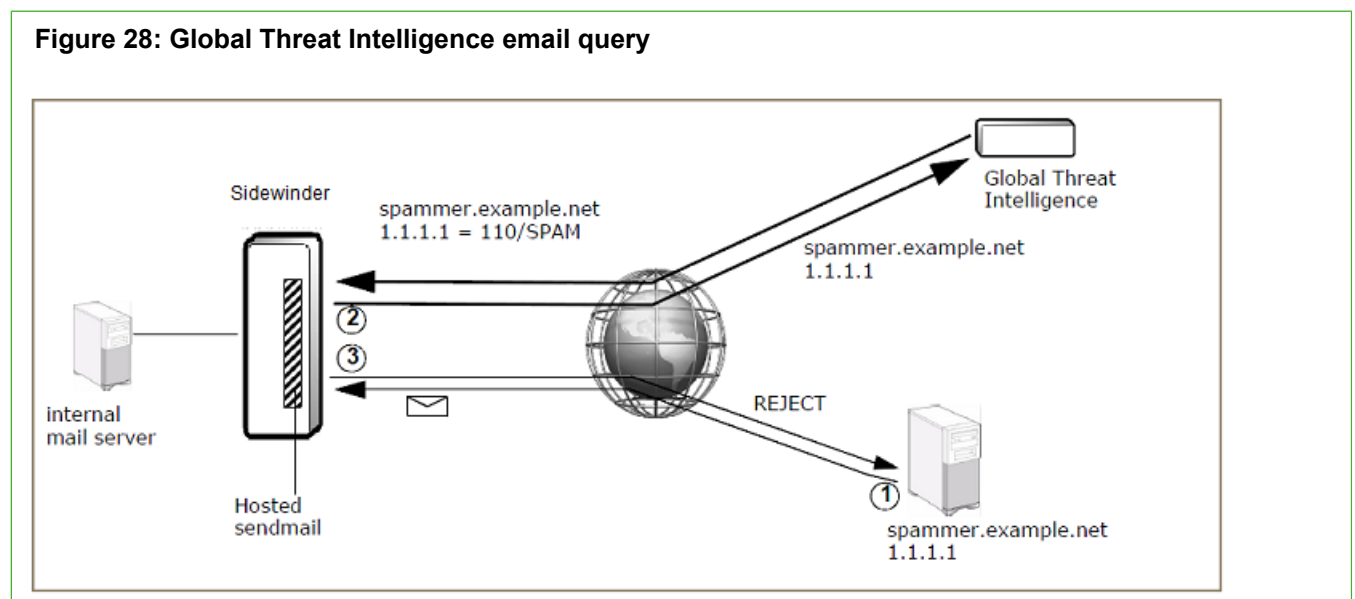


Tip: If you want to use Global Threat Intelligence to filter mail and you are not currently using sendmail, we recommend enabling Global Threat Intelligence Reputation on SMTP application access control rules.

Global Threat Intelligence with sendmail works like a real-time blackhole list. You can configure what Global Threat Intelligence Reputation score is a tolerable threshold for your network. When Global Threat Intelligence filtering is enabled for sendmail, incoming mail is processed as follows:

- 1) A sending server contacts a firewall running hosted sendmail.
- 2) The firewall sends a modified DNS query to a Global Threat Intelligence server to get the reputation score for the sending server's IP address.
- 3) The firewall compares the score to the configured threshold value.
 - If the score is lower than the threshold, the firewall accepts email messages from the server.
 - If the score is higher than the threshold, the firewall rejects the message, audits the violation, and closes the connection.

Figure 28: Global Threat Intelligence email query



Related concepts

[Using Global Threat Intelligence in access control rules](#) on page 130

[Configure Global Threat Intelligence filtering for sendmail](#) on page 135

Configure Global Threat Intelligence settings

To configure Global Threat Intelligence settings for access control rules and email filtering, select **Policy > Application Defenses > GTI Reputation**. The **GTI Reputation** window appears.



Tip: For option descriptions, click **Help**.

Related concepts

[Configure Global Threat Intelligence filtering for sendmail](#) on page 135

Related tasks

[Configure Global Threat Intelligence settings for access control rules](#) on page 133

Configure Global Threat Intelligence settings for access control rules

Global Threat Intelligence is used in access control rules to examine reputation scores of IP addresses for inbound and outbound traffic.

You can perform these actions on the GTI Reputation window:

Create a Global Threat Intelligence whitelist

In the **Global Threat Intelligence Whitelist** area, select objects to include in the Global Threat Intelligence whitelist.

Selected objects are not examined for Global Threat Intelligence reputation scores and are exempt from access control rule Global Threat Intelligence matching requirements.

- **Add object types to the whitelist.**

To include all objects of a type in the Global Threat Intelligence whitelist, select the object in the **Do not perform GTI on these objects** list.

Some objects are selected by default because your security policy most likely defines allow and deny access control rules for these objects.

To exclude an object type from the Global Threat Intelligence whitelist, clear the object's check box. All objects of that type are included in Global Threat Intelligence queries and are subject to Global Threat Intelligence matching in access control rules.

- **Add individual objects to the whitelist.**

- 1) Clear the object type in the **Do not perform GTI on these objects** list.

- 2) Click **Edit** and select objects that you want to whitelist in the pop-up window.
- **Select zones to be examined by Global Threat Intelligence.**
Select zones to exclude from the whitelist. These zones are examined by Global Threat Intelligence and are subject to Global Threat Intelligence matching in access control rules.
 - You might want to have external zones and internal zones with routable IP addresses evaluated by Global Threat Intelligence.
 - Private IP addresses are not evaluated by Global Threat Intelligence or examined in access control rules (for example, 10.x.x.x, 172.16.x.x, 192.168.x.x).

To exclude zones from the whitelist:

- 1) Select **Zones except the following**.
- 2) Select zones to exclude from the whitelist:
 - To exclude a single zone, select it from the drop-down list.
 - To exclude multiple zones, click **Choose zones to add to GTI whitelist (...)**, then select zones from the pop-up window.

Include audit for allowed traffic

Select the **Audit traffic allowed by GTI** check box to include the reputation scores of an allowed connection's IP addresses in the audit log.

If the check box is selected and Global Threat Intelligence is used to look up the reputation of the source and/or destination IP address of a connection that is allowed, it appears in the audit log like this example:

```
dest_reputation: 20
```

An allow audit message appears in the audit log only if Global Threat Intelligence was used in the access control rule matching process. It will not appear in the audit log for allowed connections under these conditions:

- Both the source and destination IP addresses are on the Global Threat Intelligence whitelist.
- The connection is allowed by an access control rule that is positioned before another access control rule that uses Global Threat Intelligence.
- The connection does not match another element in the access control rule using Global Threat Intelligence (for example, the destination zone did not match), but is allowed by a subsequent access control rule that does not use Global Threat Intelligence.

Query a host's reputation

Use the **Tools** area to directly query a host's reputation on the Global Threat Intelligence website.

Steps

- 1) In the **Host** field, type the host name.



Tip: For option descriptions, click **Help**.

- 2) Click **Query**. A Global Threat Intelligence Feedback web page for the specified host opens.

Adjust reputation boundaries

You can adjust the reputation boundaries and the default reputation if Global Threat Intelligence servers are unavailable. If you want to revert to the original settings, click **Restore Defaults**.

Configure Global Threat Intelligence filtering for sendmail

If you are using sendmail, you can enable Global Threat Intelligence filtering.



Tip: If you want to use Global Threat Intelligence to filter mail and you are not currently using sendmail, we recommend enabling Global Threat Intelligence Reputation on SMTP application access control rules.

Related concepts

[Using Global Threat Intelligence with sendmail](#) on page 132

[Using Global Threat Intelligence in access control rules](#) on page 130

Enable Global Threat Intelligence for sendmail

Enable Global Threat Intelligence email filtering.

Steps

- 1) Select **Perform GTI filtering on inbound mail**.



Tip: For option descriptions, click **Help**.

- 2) In the **Reputation threshold** field, specify a threshold. Messages from senders with reputation scores above that value are rejected.
 - Valid threshold values are 0 –120.
 - The default threshold is **80**.



Note: Trustworthy senders receive low scores and untrustworthy senders receive high scores. For reference, compare the reputation threshold to the configured reputation boundaries in the **Advanced Settings** area.

- 3) Save your changes.

Result

The firewall now uses the Global Threat Intelligence reputation service to filter inbound email.

Blackhole senders with ratings above the configured reputation threshold

We recommend that in addition to enabling Global Threat Intelligence filtering, you configure an attack response that is triggered by the audit violation and that blackholes all traffic coming from the untrusted server.

In addition to silently dropping that host's incoming connections, blackholing immediately closes all existing connections with that host. This is particularly useful if the sender's reputation score was updated after the spam flood began.

Steps

- 1) Select **Monitor > Attack Responses**.
- 2) Select the **Global Threat Intelligence** attack response.



Tip: For option descriptions, click **Help**.

Its preconfigured settings are:

- **Attack Frequency** — Always Respond
- **Alerts** — Send email, and wait 120 seconds between alerts
- **Strikeback** — Blackhole each host responsible for 100% of the attacks for 21600 seconds (6 hours)

- 3) Right-click the Global Threat Intelligence attack response and select **Enable**.
- 4) Save your changes.

Result

The firewall now blackholes hosts that have Global Threat Intelligence reputation scores that do not meet the set threshold and are trying to send email to your network. Use the Blackholed IPs feature on the Dashboard to manage blackholed IP addresses.

Benefits of SmartFilter

SmartFilter is a web filtering solution designed to manage access to the Internet.

Using SmartFilter mitigates your organization's exposure to viruses, malware, and other security risks while reducing legal liability, maximizing employee productivity, and preserving bandwidth for business-related activities.

SmartFilter uses a database of millions of URLs that are categorized based on their content. Category examples include Gambling, General News, and Online Shopping. SmartFilter manages web access at several levels, ranging from simple access restrictions for specific sites to thorough blocking of all websites categorized as unproductive or non-business-related.

To filter web traffic using SmartFilter, you must:

- 1) Choose a management method.
- 2) Configure a SmartFilter management method.

- Manage SmartFilter using the firewall Admin Console
- Manage SmartFilter using the SmartFilter Administration Console



Note: This is a legacy feature and is not actively supported.

- 3) Enable SmartFilter on the appropriate access control rules.

Related concepts

[SmartFilter management options](#) on page 137

Related tasks

[Manage SmartFilter using the firewall Admin Console](#) on page 139

[Enable SmartFilter on an access control rule](#) on page 144

SmartFilter management options

Two management methods are available when using SmartFilter with Sidewinder.

- **Firewall Admin Console** — Use the Sidewinder Admin Console to manage SmartFilter policy; this option provides reduced functionality.
- **SmartFilter Administration Console** — Use the SmartFilter Administration Console, which is installed on a standalone computer, to manage SmartFilter policy.



Note: This is a legacy feature and is not actively supported.

Related concepts

[Firewall Admin Console](#) on page 137

[SmartFilter Administration Console](#) on page 138

Firewall Admin Console

When managing SmartFilter using the Sidewinder Admin Console, basic functionality is available.

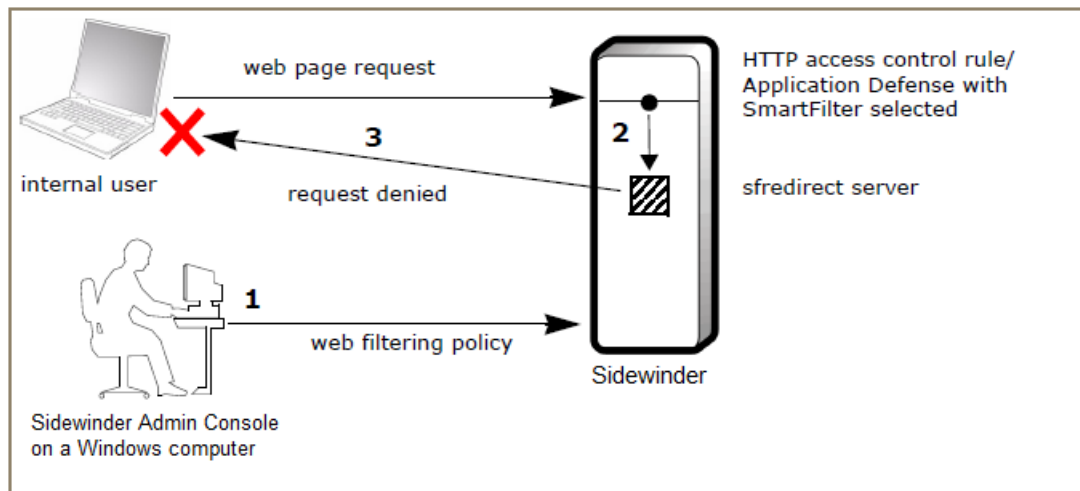
You can:

- Create filter policy.
- Define custom categories and sites.
- Pre-filter HTTP requests using Global Threat Intelligence web reputation.
- Require Google and Yahoo! SafeSearch.
- Audit SmartFilter events to local files or McAfee Web Reporter.



Note: McAfee Web Reporter is a legacy feature and is not actively supported.

Figure 29: Firewall Admin Console web filtering process



The following actions take place in the preceding figure:

- 1) SmartFilter filtering policy is configured using the Sidewinder Admin Console.
- 2) Sidewinder checks users' web requests and allows or denies the requests based on that policy.
- 3) If a connection is not allowed, SmartFilter sends an access denied message to the user making the request.

To configure this management method, see *Manage SmartFilter using the firewall Admin Console*.

Related tasks

[Manage SmartFilter using the firewall Admin Console](#) on page 139

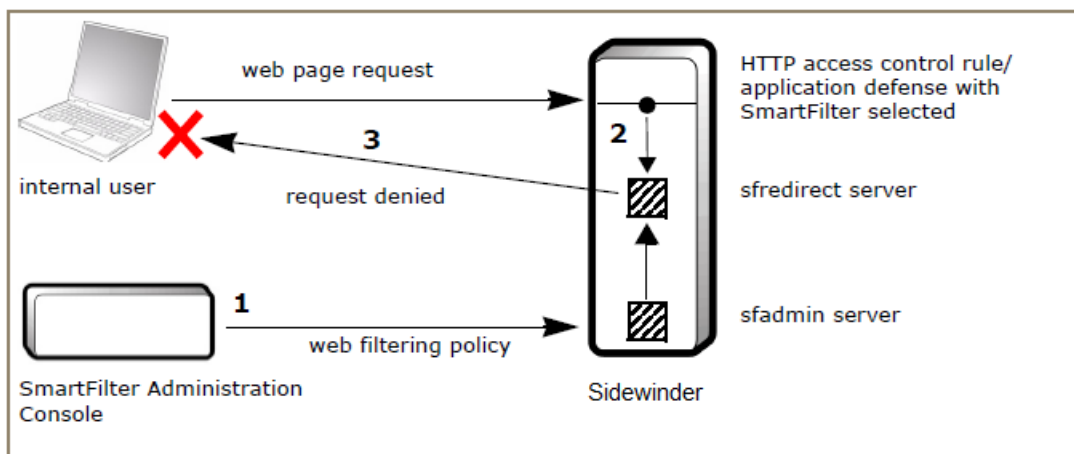
SmartFilter Administration Console

The SmartFilter Administration Console software provides full web filtering functionality and must be installed on a standalone computer.



Note: The SmartFilter Administration Console does not support IPv6.

Figure 30: SmartFilter Administration Console web filtering process



The following actions take place in Figure 8-57:

- 1) SmartFilter sends the filtering policy to the Sidewinder sfadmin server.
- 2) Sidewinder checks users' web requests and allows or denies the requests based on that policy.
- 3) If a connection is not allowed, SmartFilter sends an access denied message to the user making the request.

Manage SmartFilter using the firewall Admin Console

Manage SmartFilter in the firewall Admin Console.

Perform the following procedures:



Tip: To filter web traffic using SmartFilter, you must enable it on the appropriate access control rule(s). See *Enable SmartFilter on an access control rule*.

Related tasks

[Enable SmartFilter on an access control rule](#) on page 144

Enable firewall Admin Console SmartFilter management

To manage SmartFilter using the firewall Admin Console.

Steps

- 1) Select Policy > Application Defenses > SmartFilter.

- 2) On the **SmartFilter Management** tab, select **Firewall Admin Console or Control Center**.



Tip: For option descriptions, click **Help**.

- 3) [Optional] Configure the URL requests by IP address to specify the filter action for uncategorized URLs.
- 4) [Conditional] If SmartFilter was not bundled with your firewall and you purchased SmartFilter separately, specify your SmartFilter serial number.
 - a) Select **Use alternative license for 7X upgraded firewalls**.
 - b) Type your SmartFilter serial number in the **Activate SmartFilter for 8X Firewall using serial number** field.
- 5) Save your changes.

Download URL category updates

To ensure that the URL categories used by SmartFilter to filter web traffic are up to date, the firewall must periodically download category updates from the Global Threat Intelligence Web Database, XL version.

Download URL categories and configure URL category updates.

Steps

- 1) Select **Maintenance > Updates**.
- 2) In the upper pane, select **SmartFilter updates**.
 - a) Click **Update Database Now**. A pop-up window appears.
 - b) Click **Background** or **Wait**. The firewall downloads the URL categories.
- 4) Select **Enable automated updates**, then specify the update frequency.



Tip: We recommend configuring **Daily** or **Realtime** updates.

- 5) Save your changes.

Related tasks

[Manage service updates](#) on page 600

Configure filter policies

Use filter policies to configure web filtering based on your organization's acceptable use policy.

To apply a filter policy to an access control rule, select the filter policy on the access control rule's Application Defense.


To configure filter policies for SmartFilter, select **Policy > Application Defenses > SmartFilter**, then click the **Filter Policies** tab.




Tip: For option descriptions, click **Help**.

You can perform the following tasks:

Table 33: Filter policy management tasks

Task	Steps
Create a new filter policy	<ol style="list-style-type: none"> 1) Click Create a new filter policy. The Filter Policy window appears. 2) In the Filter Policy window, configure the fields as necessary. 3) Click OK, then save your changes.
Modify a filter policy	<ol style="list-style-type: none"> 1) Select the filter policy that you want to modify, then click Modify a filter policy. The Filter Policy window appears. 2) In the Filter Policy window, update the filter policy as necessary. 3) Click OK, then save your changes.
Delete a filter policy	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Note: The default filter policies cannot be deleted.</p> </div> </div> <ol style="list-style-type: none"> 1) Select the filter policy that you want to delete, then click Delete a filter policy. A confirmation pop-up appears. 2) Click Yes, then save your changes.
Duplicate a filter policy	Select the filter policy that you want to duplicate, then click Duplicate a filter policy . A duplicate of the filter policy appears, named <code>Copy_of_<policy_name></code> .

Task	Steps
Rename a filter policy  Note: The default filter policies cannot be renamed.	<ol style="list-style-type: none"> 1) Select the filter policy that you want to rename, then click Rename a filter policy. The Rename Policy window appears. 2) In the Rename Policy window, type a new policy name. 3) Click OK, then save your changes.
Search filter policies	Type a search term in the Find field.

Customize sites

Create custom sites to recategorize URLs according to your organization's acceptable use policy.

For example, if SmartFilter categorized <http://www.example.com> as Entertainment, you could recategorize it as Alcohol by creating a custom site.



Note: If a URL categorized in the Internet Database is recategorized using Custom Sites, the Custom Sites categorization takes precedence.

You can add custom sites to the default categories, or you can create custom categories. Filter policy action is configured at the category level, not the site level.

To define custom categories and sites, select **Policy > Application Defenses > SmartFilter**, then click the **Custom** tab.




Tip: For option descriptions, click **Help**.

Use the table to perform tasks on the **Custom** tab.

Table 34: Custom category and site management tasks

Task	Steps
Create a new category	<ol style="list-style-type: none"> 1) In the Categories toolbar, click New category. The Custom: New Category window appears. 2) In the Custom: New Category window, specify a new category name. 3) Click OK, then save your changes.

Task	Steps
Delete a category  Note: The default categories cannot be deleted.	<ol style="list-style-type: none"> 1) Select the category you want to delete. 2) Delete all of the custom sites in the category. 3) Click Delete category. A confirmation pop-up appears. 4) Click Yes, then save your changes.
Search categories	In the Categories toolbar, type a search term in the Find field.
Create a new site	<ol style="list-style-type: none"> 1) Select the category that you want to add the site to. 2) In the Custom sites toolbar, click New site. The Custom: New Site window appears. 3) In the Custom: New Site window, specify a URL. 4) Click OK, then save your changes.
Delete a site	<ol style="list-style-type: none"> 1) Select the category that contains the site you want to delete. 2) Select the site you want to delete, then click Delete site. 3) Save your changes.
Search sites	<ol style="list-style-type: none"> 1) Select the category you want to search. 2) In the Custom sites toolbar, type a search term in the Find field.

Configure SmartFilter auditing

You can configure SmartFilter to create an audit entry for each HTTP request it filters.

SmartFilter audits can be sent to:

- **Log files on the firewall** — SmartFilter audits are written to the following log files:
 - /var/log/audit.raw
 - /var/log/SF.log
- **McAfee Web Reporter** — SmartFilter audits are sent to reporting software that is installed on a standalone computer, which provides the reporting tools needed to help you identify issues such as:
 - Liability exposure

- Productivity loss
- Bandwidth overload
- Security threats



Note: This is a legacy feature and is not actively supported.

To configure SmartFilter auditing, select **Policy > Application Defenses > SmartFilter**, then click the **Audit** tab.



Tip: For option descriptions, click **Help**.

To enable SmartFilter auditing:

Steps

- 1) Select **Enable SmartFilter auditing**.
- 2) In the **Audit destination** area, configure where you want SmartFilter audits to be sent.
- 3) [Conditional] If you select **Remote report server** or **Both**, complete the **Report server address** and **Port** fields.

Enable SmartFilter on an access control rule

Enable SmartFilter web filtering enforcement on access control rules.

To enable SmartFilter on an access control rule, you must first configure a SmartFilter management method. See:

- *Manage SmartFilter using the firewall Admin Console*
- *Manage SmartFilter using the SmartFilter Administration Console*

To enforce SmartFilter web filtering on an access control rule:

Steps

- 1) Configure SmartFilter on the appropriate HTTP Application Defense:
 - a) Select **Policy > Application Defenses > Defenses > HTTP**.
 - b) Select an existing Application Defense, or create a new one.



Tip: For option descriptions, click **Help**.

- c) On the **Enforcements** tab, select **SmartFilter**.
- d) Click the **SmartFilter** tab, then configure it as appropriate.
 - To deny all HTTP requests that occur when SmartFilter is not available, select **Reject all requests if SmartFilter is unavailable**.
 - [Firewall Admin Console-managed SmartFilter] From the **Filter Policy** drop-down list, select the filter policy you want to apply to the access control rule.

- e) Save your changes.
- 2) Configure an Application Defense group.
 - a) Select **Policy > Application Defenses > Defenses > Groups**. The **Groups** window appears.
 - b) Create a new Application Defense group or modify an existing Application Defense group.
 - c) In the list of Application Defenses for this group, select the HTTP application defense you configured in step 1.
 - d) Save your changes.
 - 3) [Optional] To enable web filtering for HTTPS connections, do one of the following:
 - Create an outbound decrypt/re-encrypt SSL rule to inspect HTTPS connections.
 - Allow non-transparent HTTP connections by modifying the Generic Application Defense in the Application Defense group you configured in Step 2.



Note: This method does not filter transparent HTTPS connections.

- 4) Modify the appropriate access control rule.
 - a) Select **Policy > Access Control Rules**.
 - b) Open the appropriate access control rule or create a new one.



Note: SmartFilter is applied to only the HTTP-based Applications.

- c) From the **Application Defense** drop-down list, select the Application Defense group you configured in step 2.
- d) Close the access control rule, then save your changes.

Related concepts

- [Configuring access control rules on page 197](#)
- [Managing Application Defense profiles on page 191](#)

Related tasks

- [Manage SmartFilter using the firewall Admin Console on page 139](#)

McAfee EIA

Contents

- [How McAfee EIA works](#) on page 147
- [Benefits of McAfee EIA](#) on page 149
- [Understanding file reputation in the firewall audit](#) on page 150
- [Configure certificates](#) on page 152
- [Configure McAfee EIA settings on Sidewinder](#) on page 156
- [View active hosts connected to Sidewinder](#) on page 163
- [View related firewall audit](#) on page 164

McAfee® Endpoint Intelligence Agent (McAfee EIA) is an endpoint solution that provides per-connection information to Sidewinder.

How McAfee EIA works

McAfee EIA sends connection information, called *metadata*, that Sidewinder uses for policy decision making and auditing.

When McAfee EIA is installed on a host system, it monitors the system for any outgoing connections. When a connection attempt is made, the agent sends the following information to Sidewinder over an encrypted channel.



Note: If the metadata sent by McAfee EIA has UTF-8 characters in any of the attributes, the characters might not display properly in the Admin Console **Audit Viewer** or **Dashboard** windows.

- Source and destination address
- Protocol
- Source and destination port
- The user information associated with the process
- The executable file name on disk, full path
- Executable file information (only suspicious DLL files are included)
 - MD5 hash value
 - File description
 - File signer
 - File signed time
 - File name (name from version table)
 - File version
 - Product name
 - Malware analysis information
 - Malware risk level

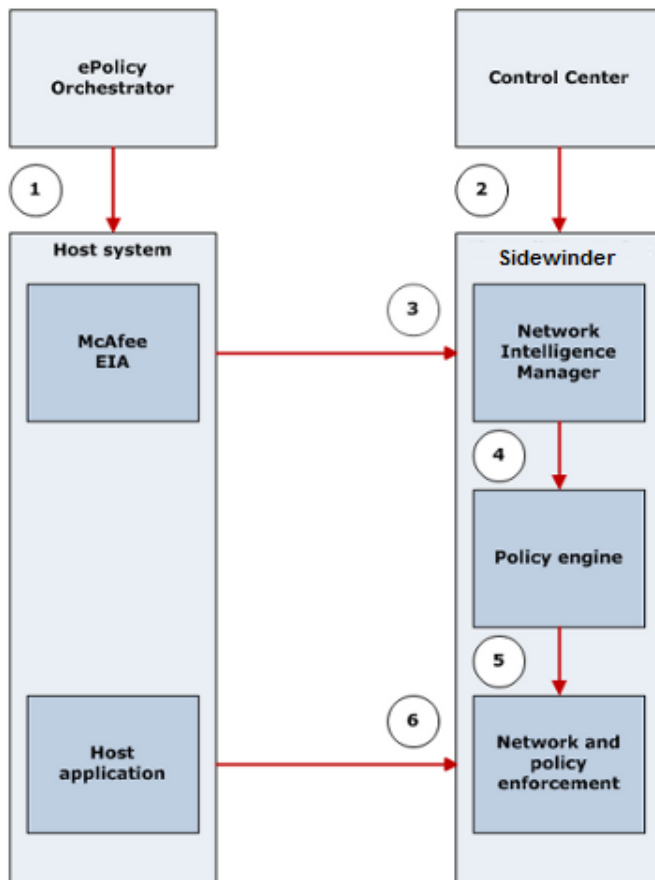
- Heuristics
- Evidence data



Note: McAfee EIA currently provides metadata for TCP and UDP connections over IPv4.

McAfee EIA is managed by McAfee ePolicy Orchestrator and can be deployed to multiple systems.

Figure 31: Integrating McAfee EIA with Sidewinder



- 1) McAfee ePolicy Orchestrator installs and configures McAfee EIA on managed hosts.
- 2) Sidewinder is configured for McAfee EIA using the Admin Console. If your firewall is managed by Control Center, the firewall is configured on the Control Center Management Server.
- 3) McAfee EIA sends metadata to Sidewinder.
- 4) User information is used for authentication and policy enforcement. User information and other metadata is used for auditing.
- 5) Firewall policy is applied.
- 6) The host system initiates the network connection for the application. Sidewinder allows or denies the connection based on its policy.



Note: McAfee EIA works with enterprise point product installations on the host machines. Consumer point product installations are not supported.

Benefits of McAfee EIA

McAfee EIA collects user information associated with an application and sends metadata to the firewall.

Many network environments contain computers or servers that have multiple users logged on at the same time. The user information in the metadata allows the firewall to determine what users are associated with what connections, even if those connections are coming from the same IP address.

You can view the information collected by McAfee EIA in the firewall audit, providing better visibility on what users and applications are initiating connections on your network.

The metadata gathered from the host, Global Threat Intelligence, and the classification list maintained on the firewall is used to calculate the overall confidence score of an executable file connection. The firewall audits executable file connections, and attack responses can be configured for malicious or unknown executables.

Related concepts

[Authentication options](#) on page 156

[How McAfee Global Threat Intelligence works](#) on page 128

Related tasks

[View related firewall audit](#) on page 164

[Configure the executable file reputation capability](#) on page 158

Understanding file reputation in the firewall audit

The firewall, McAfee EIA, and Global Threat Intelligence combine to process executable file connections coming through the firewall for file reputation.

When a connection is made through the firewall, McAfee EIA supplies the executable file information in metadata. The firewall checks the executable file MD5 hash value against the Global Threat Intelligence server and any entries on the classification list.

Overall malware confidence is calculated from these elements.

- McAfee EIA on the host assigns the executable file MD5 a risk level rating: very low, low, medium, high, very high, or unknown.
- When Global Threat Intelligence is enabled, the risk level in the database is reported back to the firewall: very low, low, medium, high, very high, or unknown.
- When the classification list is enabled, the executable file is compared to the imported standard or entries manually created by the administrator.

The classification type is divided into these categories:

- **Whitelist** — When the connection has a whitelist reputation, the connection is audited and the firewall continues to process it.
- **Blacklist** — When the connection has a blacklist reputation, the connection is audited. If an attack response is configured, the firewall can send an alert or blackhole the source IP address of the connection.

In the firewall audit, you can review the specific evidence that contributed to the overall confidence score. The audit entries with an McAfee EIA correlation ID have additional audit fields: **Host_heuristic** and **Host_evidence**.

- The **Host_heuristic** audit field displays serial numbers assigned to specific types of host heuristics.
- The **Host_evidence** audit field provides a detailed description of the evidence string row text, such as the number of DLLs found or executable file sections.

Table 35: Host heuristic name and string format

Heuristic ID number	Description and format
1	Global Threat Intelligence has assigned this executable file a [Medium High Very High] malware confidence.
2	File signed information.
3	An executable file is typically linked to numerous libraries. This executable file is linked to an unusually small number of libraries.
4	An executable file typically has a resource section, which contains icons, menus, dialog boxes, and more. This executable file does not have a resource section.
5	An executable file does not typically embed another executable file. An embedded executable file has been detected in the resource section of this executable file.
6	An executable file does not typically embed a combination of unknown and encrypted information in its resource section. This executable has unknown and encrypted information embedded in its resource section.

Heuristic ID number	Description and format
7	Malware is often encrypted or packed (compressed and encrypted) to avoid detection. This executable is encrypted or packed.
8	An executable file is typically made up of read-only executable sections only. This executable file has a writeable executable section.
9	An executable file is typically made up of one or two executable sections only. This executable file has an unusually large number of executable sections.
10	An executable file typically starts its code execution from within its default executable section. This executable file is using an entry point outside its default executable section.
11	The raw data size of a file section indicates its disk footprint. Malware often sets this value to 0 to confuse debuggers and avoid detection. This executable has a section whose size is set to 0.
12	The file version name defined in the resource section of this executable file is different from the executable file's actual file name.
13	This executable file is being run from a suspicious location on the file system, such as a temp folder.
14	This executable file is associated with autorun entries in the registry.
15	This executable file is using one or more APIs often used by malware to hamper analysis and avoid detection.
16	A compiler typically generates standard section names (such as .code, .data, .bss) when it creates an executable file. This executable file has non-standard section names.
17	A compiler typically generates standard section names (such as .code, .data, .bss) when it creates an executable file. This executable file has non-standard section names.
18	Data located after the last section of an executable file is overlay data, which is an easy target for malware writers. This executable file has obfuscated overlay data.
19	This executable file has its hidden file attribute set.
20	This executable file is in the Portable Executable (PE) format, but it has a non-PE file extension (such as .jpg, .doc, .pdf).
21	This executable file has the same file name as a common Windows executable file, but is running from a non-standard folder.

Each heuristic ID number is assigned a result in the **Host_heuristic Detail View** window.

Table 36: Host heuristic results

Heuristic	Result
ID 1 GTI	Not Available — Global Threat Intelligence was not found

Heuristic	Result
ID 2 File signed	<ul style="list-style-type: none"> • Not Available — Signed file was not found • Available, not used — Signed file was not used
ID Numbers 3–21	<ul style="list-style-type: none"> • Ignored — Heuristic ignored • Skipped — Not able to calculate Heuristic, possible error in the computation • Not applicable — Heuristic computation results negative • Applicable — Heuristic computation passed

Related tasks

[Configure the executable file reputation capability](#) on page 158

[View related firewall audit](#) on page 164

Configure certificates

Certificate configuration is necessary for the encrypted communication between Sidewinder and McAfee EIA.



Note: If you are using Control Center to manage your firewall, see the *Forcepoint Sidewinder Control Center Product Guide, Certificates* chapter.

The certificate process consists of these high-level steps:


- 1) In the firewall, generate and export the certificate for McAfee EIA.
- 2) Sign that certificate in the Endpoint Intelligence Management extension.
- 3) Export the ePolicy Orchestrator certificate authority (CA) certificate.
- 4) Load the signed certificate and the CA certificate into the firewall.

When creating certificates, they must meet these requirements:

- Public key lengths must be 4096 bits or lower.
- The host certificate used by McAfee EIA must be signed by the same certificate authority that generated the CA certificate.

Generate the firewall certificate

Create and export a firewall certificate to be signed by ePolicy Orchestrator.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.


- 1) From the Sidewinder Admin Console, select **Maintenance > Certificate/Key Management > Firewall Certificates**.
- 2) Click **New**. The **Firewall Certificates: Create New Certificate** window appears.
- 3) In the **Certificate name** field, enter a name for the certificate.
- 4) In the **Distinguished name (DN)** field, enter a distinguished name.
- 5) From the **Submit to CA** menu, select **Manual PKCS 10**.
- 6) Click **Browse** to specify the name and location to export the certificate to.
- 7) From the **Format** menu, select **PKCS10**.
- 8) Click **Add**. A success message appears.
- 9) Click **OK**.

Result

The certificate is exported to the specified location.

Sign the firewall certificate and export the CA certificate

Use ePolicy Orchestrator to sign the firewall certificate and export the ePolicy Orchestrator CA certificate.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) From the ePolicy Orchestrator console, select **Menu > Configuration > Server Settings**. The **Server Settings** area appears.
- 2) Select **Network Integrity Settings**, then click **Edit**. The **Edit Network Integrity Settings** page appears.
- 3) Click **Browse** and select the firewall certificate.
- 4) Click **Sign certificate**. When prompted, specify the name and location, and save the signed certificate.

- 5) Download the ePolicy Orchestrator CA certificate.
 - a) On the **Edit Network Integrity Settings** page, click **Download extension self signed cert**.
 - b) When prompted, specify the name and location, and save the CA certificate.

Load the certificates

Load the signed certificate and the ePolicy Orchestrator CA certificate to Sidewinder.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) From the Sidewinder Admin Console, select **Maintenance > Certificate/Key Management**.
- 2) Load the signed certificate.
 - a) Click the **Firewall Certificates** tab.
 - b) In the **Certificates** list, select the certificate, then click **Load**. The **Firewall Certificates: Load Certificate for PKSC10 Request** window appears.
 - c) For **Certificate Source**, select **File**.
 - d) Click **Browse** and select the signed certificate file.
 - e) Click **OK**.
 - f) In the **Firewall Certificates** tab, select the certificate and verify the status is **SIGNED**.
- 3) Load the ePolicy Orchestrator CA certificate.
 - a) Click the **Certificate Authorities** tab.
 - b) Click **New > Single CA**. The **Certificate Authorities: New Certificate Authority** window appears.
 - c) In the **Name** field, enter a name for the certificate.
 - d) Click **Browse** and select the CA certificate file.
 - e) Click **Add**.

Configure certificates using SCEP

If you do not want to use the ePolicy Orchestrator CA to sign the certificate, you can use the Simple Certificate Enrollment Protocol (SCEP) instead.

Steps

- 1) On the ePolicy Orchestrator console, select **Menu > Configuration > Server Settings**. The **Server Settings** area appears.
- 2) Select **Endpoint Intelligence Settings**, then click **Edit**. The **Edit Endpoint Intelligence Settings** page appears.
- 3) Configure SCEP settings.
 - a) Select **CA Certificate**.
 - b) Enter the information in the **CA SCEP Url**, **CA Id** and **Scep Password** fields.
 - c) Click **Test Connection** to verify the information. A success message appears.
 - d) Click **Get CA Cert**.
- 4) On the Sidewinder Admin Console, select **Maintenance > Key Management**.
- 5) Configure the CA certificate.
 - a) Click the **Certificate Authorities** tab.
 - b) Click **New**. The **Certificate Authorities: New Certificate Authority** window appears.
 - c) From the **Type** drop-down list, select **SCEP**.
 - d) Enter the information for the CA certificate.
 - e) Click **Add**.
 - f) Click **Get CA Cert** to get the Distinguished Name details.
- 6) Configure the firewall certificate.
 - a) Click the **Firewall Authorities** tab.
 - b) Click **New**. The **Firewall Certificates: Create New Certificate** window appears.
 - c) From the **Submit to CA** drop-down list, select the name of the CA certificate you configured on the firewall.
 - d) Click **Add**.
 - e) Enter the information for the certificate.
- 7) Save your changes.

Configure McAfee EIA settings on Sidewinder

Use the Admin Console to configure McAfee EIA settings.

For more information on installing and setting up McAfee EIA, see the *McAfee Endpoint Intelligence Agent Installation Guide*.

Authentication options

Sidewinder works with Logon Collector to enforce policy based on the user information provided by McAfee EIA.

You can configure authentication settings for McAfee EIA using these methods:

- **Authentication disabled** — User information provided in the metadata is not used to enforce policy. It is used for auditing purposes only.
- **Authentication enabled** — User information provided in the metadata is used for policy enforcement and auditing purposes. When authentication is enabled, you determine the mode to use when the firewall does not receive valid user information. This happens if the metadata does not contain a user that is part of a Windows Domain or if the firewall does not receive any metadata for the connection.
 - **Authentication with fallback to Logon Collector** — When no valid user information is provided, use authentication information provided by Logon Collector to enforce policy on the connection.
 - **Authentication without fallback to Logon Collector** — When no valid user information is provided, do not use authentication information provided by Logon Collector. The connection will not match any rules that require authentication.



Note: Passive Passport must be enabled to use McAfee EIA authentication.

Configure authentication and certificate settings

Specify the certificates to use for the communication with McAfee EIA, and determine the authentication method to use.



Note: If you want to specify the zones and endpoints McAfee EIA responds to, create an explicit McAfee EIA communication rule before enabling McAfee EIA on the firewall.

Steps

- 1) Select **Policy > Rule Elements > EIA**. The **General Settings** tab appears.



Tip: For option descriptions, click **Help**.

- 2) Select **Enable Endpoint Intelligence Agent**.

- 3) In the **Shared Key** field, type the shared key used in the communication between Sidewinder and McAfee EIA.
- 4) [Optional] Enable authentication.



Note: Passive Passport must be enabled to use McAfee EIA authentication.

- a) Select **Enable**.
- b) Select the method of authentication from the **Mode** menu. This mode determines if Sidewinder will fall back on Logon Collector authentication in the event that it is not possible to provide user information, such as users that are not part of a Windows Domain, or if metadata is not received.
 - **Do not fallback to Logon Collector** — Select **eia**.
 - **Fallback to Logon Collector** — Select **fallback_mlc**.
- 5) From the **CA Certificate** menu, select the SCEP or ePolicy Orchestrator CA certificate.
- 6) From the **Firewall Certificate** menu, select the firewall certificate you created on the firewall previously.
- 7) [Optional] Configure certificate revocation and expired certificate settings.
- 8) Save your changes.

Related tasks

[Create an explicit McAfee EIA communication rule](#) on page 162

Sidewinder discovery options

McAfee EIA hosts can dynamically discover the gateway firewall for a given route.

When a connection attempt is made, McAfee EIA determines if there is a firewall gateway configured for that route. If there is, the agent sends metadata to the specified firewall IP address. If there is no firewall configured for that route, the agent does not send metadata.

If agent discovery is enabled and the firewall receives a connection from a host without any metadata, it uses the *Selected objects enabled/disabled for discovery* list in the **Hosts and Discovery** tab to determine if the firewall will send a message to the McAfee EIA running on the host. This message tells the agent to send metadata to the firewall before sending the actual connection.

- If the *Selected objects enabled/disabled for discovery* list is empty, the firewall always sends a message to any host that does not send metadata.
- IP address, IP address range, and subnet objects can be specified in the *Selected objects enabled/disabled for discovery* list. The firewall only sends messages to objects that are present and enabled in the list. The firewall processes disabled entries in the list before processing enabled entries.

Example: Assume you have network objects for the subnet 10.1.1.0/24 and the host 10.1.1.25. You want the firewall to send the metadata request message to all devices on the 10.1.1.0/24 subnet except for 10.1.1.25, because it is a device (such as a printer or Linux server) that does not have the agent installed. In this case, you would add both network objects to the *Selected objects enabled/disabled for discovery* list, but you would only enable the object for 10.1.1.0/24. The object for 10.1.1.25 would remain disabled.

Configure agent discovery

Enable and configure discovery options on Sidewinder.

Steps

- 1) Select **Policy > Rule Elements > EIA**.
- 2) Click the **Hosts and Discovery** tab.



Tip: For option descriptions, click **Help**.

- 3) Select **Enable Discovery**.
- 4) From the **Select network objects for discovery lists** list, select the network objects to configure for discovery.
- 5) In the **Enable / Disable** column of the *Selected objects enabled/disabled for discovery* list, select the network objects you want the firewall to send the metadata request message to.
- 6) Save your changes.

Configure the executable file reputation capability

You can enable the firewall to accept and respond to the executable file reputation data received from McAfee EIA and Global Threat Intelligence.

To implement a standard for endpoint hosts, generate an .xml file of the executable file MD5 hash values using the Endpoint Baseline Generator, import the file into the firewall, then enable McAfee EIA to report any deviations from that standard.

You can configure responses for these scenarios:

- A new executable file is detected.
Unknown executable files are captured in the audit. You can set up an attack response to send an alert or strikeback.
- A blacklist executable file is detected.
You can identify vulnerable application versions as blacklisted on the classification list. You can set up an attack response to send an alert or strikeback.


Enable Global Threat Intelligence for executable files

When enabled, executable file connections from the host are compared to the Global Threat Intelligence reputation database.

Before you begin

- McAfee EIA must be enabled.
- The firewall must be licensed for TrustedSource.

The firewall receives the MD5 hash value of each connection from McAfee EIA. The Global Threat Intelligence reports the reputation information about each file.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Policy > Rule Elements > EIA > Executable Reputation**.
- 2) Select **Enable Executable Reputation**.
- 3) Select **GTI Reputation**.
- 4) Save your changes.

Related tasks

[Create an attack response](#) on page 321

Enable classification list executable file reputation matching

When enabled, executable file connections from the host are compared to the reputation classification list.

Before you begin

If you are importing an executable file list, it must be an .xml file generated by the Endpoint Baseline Generator tool.



Note: The executable file names must be ASCII characters only. Using UTF-8 characters will result in an error, and the XML file will not be applied.

You can import a predefined standard executable file list, or add executable entries individually.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Policy > Rule Elements > EIA > Executable Reputation**.
- 2) Select **Enable Executable Reputation**.
- 3) Select **Classification list**.
- 4) Take one of these actions, then save your changes.

Action	Steps
Add an executable file entry	<ol style="list-style-type: none"> 1) Click New. 2) In the Executable Reputation: Add window, specify the name of the executable. 3) Enter the hash value. 4) From the drop-down list, select the type. The executable can be added to either the whitelist or blacklist. 5) Click Add. <p>The entry is added to the list.</p>
Import a list of executables files	<ol style="list-style-type: none"> 1) Click Import. 2) In the Executable Reputation: Import window, browse to the .xml file. 3) Select Add to existing list. Leaving this deselected results in the new list overwriting the existing list. 4) If this is a duplicate entry, select Ignore duplicate entries to keep entries. If this is deselected, the old executable file entry remains and the new entry is not imported. 5) Define the Whitelist and Blacklist thresholds. For example, if Whitelist is set to Low Risk, all the entries with reputation Very Low Risk, Unknown, and Low Risk go to the whitelist. If Blacklist is set to Medium Risk, all the entries with reputation Medium Risk, High Risk, and Very High Risk go to the blacklist. 6) Click OK. <p>The file is parsed and the list is generated.</p>

Action	Steps
Delete an executable file entry	<ol style="list-style-type: none"> 1) Select the executable entry to be deleted. 2) Click Delete, then click Yes to confirm the deletion. <p>The selected entry is deleted.</p>
Purge all executable file entries	<p>Click Purge, then click Yes to confirm the deletions.</p> <p>All entries are deleted.</p>
Change the type	<ol style="list-style-type: none"> 1) Select the executable entry to be changed. 2) Click Whitelist or Blacklist. <p>The entry is added to the chosen type list.</p>
Filter for specific executable file entries	<p>Enter the search criteria, then click Search or press Enter.</p>

Next steps

To configure how the firewall responds to the executable file connection reputation, you must configure an attack response.

Related tasks

[Create an attack response](#) on page 321

Modify advanced firewall settings

Optionally, you can modify advanced settings for McAfee EIA, such as the maximum number of connected hosts and connection timeouts.

Steps

- 1) Select **Policy > Rule Elements > EIA**.
- 2) Click the **Advanced Settings** tab.



Tip: For option descriptions, click **Help**.

- 3) Modify the settings as needed.
- 4) Save your changes.

Create an explicit McAfee EIA communication rule

The Network Intelligence Manager daemon (nimd) is the daemon responsible for communication with McAfee EIA. By default, nimd is enabled in all zones except the one configured as the Internet zone.

You can create a rule to specify the particular zones, source endpoints, and destination endpoints you want nimd to respond to.

This configuration is recommended, but optional.



Note: Create this rule before enabling McAfee EIA on the firewall.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type a name for the rule.
- 4) From the **Action** drop-down list, select **Allow**.
- 5) In the **Applications** pane, select **EIA Manager**.
- 6) In the **Source** area, specify the connection sources to match.
 - a) In the **Endpoints** pane, select the endpoints.
 - b) From the **Zone** drop-down list, select the zones.
- 7) In the **Destination** area, specify the connection destinations to match.
 - a) In the **Endpoints** pane, select **<Any>** or an object that contains the firewall IP address.
 - b) From the **Zone** drop-down list, select the same zones as specified in the **Source** area.
- 8) From the **NAT** drop-down list, select **<None>**.
- 9) Click **OK**.
- 10) Save your changes.

Related tasks

[Configure authentication and certificate settings](#) on page 156

View active hosts connected to Sidewinder

There are two methods of viewing active hosts connected to Sidewinder.



Note: If you are using Control Center to manage your firewall, see the *Forcepoint Sidewinder Control Center Product Guide, Generate Active Hosts Report*.

View connected hosts using the Admin Console

Use the Admin Console to view connected agent hosts.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) From the Sidewinder Admin Console, select **Policy > Rule Elements > EIA**.
- 2) Click the **Hosts and discovery** tab.

Result

The **Active Host Agents** area displays the list of connected hosts.

View connected hosts using the command line interface

Use the firewall command line interface to view connected agent hosts.

Steps

- 1) Using command line, log on to the firewall.
- 2) Type `srole` to change to the Admn domain.
- 3) Enter the command:

```
ipfilter -vH
```

Result

The list of connected hosts appears.

View related firewall audit

From the firewall dashboard, access firewall audit entries related to McAfee EIA.



Note: If you are using Control Center to manage your firewall, see the *Forcepoint Sidewinder Control Center Product Guide, View improved category reports*.

Steps

- 1) From the Sidewinder Admin Console, log on to the firewall. The dashboard appears.



Tip: For option descriptions, click **Help**.

- 2) View the list of recent audit entries for McAfee EIA.
 - a) Click the **EIA** tab. A list of recent audit entries for McAfee EIA appear.
 - b) From the drop-down list, select the amount of most frequently audited application reputations.
 - c) From the drop-down list, select either **Host-Application-Reputation** or **Malicious-Host-Application-Reputation**.
 - d) Select the time range.
 - e) Click **Go**.
 - f) Review the audit events using one of these methods:
 - Select an audit event and click **View Audit**.
 - Select a user and click **View Reputation Audits for user**.
 - Select an audit event and click **View Reputation Audits**.
 - g) In the **EIA: Audit Viewing** window, select an audit event and click **Obtain evidence provided by EIA**. The **Detail View** window appears.
 - h) You can double-click **Host_heuristic** or **Host_evidence** for more information.
- 3) View the list of recent audit entries for executable files and their Global Threat Intelligence reputations.
 - a) Click the **GTI** tab. A list of recent audit entries for Global Threat Intelligence appears.
 - b) From the drop-down list, select the amount of most frequently audited executables.
 - c) From the drop-down list, select either **Executable** or **Malicious-Executable**.
 - d) Select the time range.
 - e) Click **Go**.



Tip: To view the full audit entries, click **View Audit**.

Applications

Contents

- [Using applications in policy](#) on page 165
- [Manage applications](#) on page 173
- [Manage application groups](#) on page 175
- [Updating application signatures on an isolated network](#) on page 177

Sidewinder uses applications to classify network connections and act on them. Applications allow you to control connections based on function in addition to traditional attributes such as protocol or port.

Using applications in policy

Sidewinder uses applications to identify and enforce policy on connections.

AppPrism allows the firewall to look closely at the actual data in the application. This gives you the ability to:

- Control the traffic
- Instruct the firewall how to respond to the data
- Create custom applications and application groups for use in your policy (in addition to the application database)

For example, consider the Facebook application. Traditional firewalls have difficulty distinguishing connections to Facebook from other HTTP and HTTPS traffic. In contrast, the Sidewinder Facebook application identifies connections to Facebook without forcing you to consider connection attributes.

Applications in access control rules

Use access control rules to determine which applications are allowed and denied.

There are several ways to associate applications with an access control rule.

- **Individual applications** — Select one or more applications when you create the access control rule.
- **Application groups** — Create an application group that contains the appropriate applications, then select that group when you create the access control rule.
- **Application category filters** — [Deny and drop actions only] Select an application category filter to block all applications that belong to that category. Application categories cannot be selected for access control rules with allow action.



Note: We recommend creating specific deny rules and placing them above general allow rules for HTTP-based applications. For example, a deny Facebook rule would be placed above an allow HTTP rule.

Related concepts

[Troubleshooting applications](#) on page 669

Related information

[Creating and managing access control rules](#) on page 197

[Working with policy](#) on page 223

How applications are identified

The firewall scans deeper into the flow of data to detect applications.

McAfee AppPrism examines connection protocols and data, and matches them to application signatures to identify applications. AppPrism is the technology that allows for an application-based policy. Using SSL Content Inspection, AppPrism can even identify applications encapsulated in SSL. Each session is inspected for application information.

Sidewinder leverages the AppPrism engine to identify the application used in incoming connections. When a new connection request arrives, the firewall performs these processes.



Identify	Compare	Respond
The firewall identifies the port and protocol being used. If the protocol is SSL and decryption is enabled, the packet content is decrypted.	The AppPrism engine compares the port, protocol, and other data to its library of application signatures and identifies the application being used.	The firewall responds based on the identity of the application and the associated access control rules.

Related concepts

[McAfee AppPrism](#) on page 14

[Discovering which applications are in use in a zone](#) on page 260

Application elements

Applications consist of multiple elements that are used to classify network connections; refer to the table.

Table 37: Elements of applications

Element	Definition
Signature	Detects the application based on content or behavior.

Element	Definition
Ports	<p>Describes the ports used by the application. There are three types of ports:</p> <ul style="list-style-type: none"> • TCP — Ports of this type apply only to connections that use the TCP protocol. • SSL — Ports of this type apply only to connections that are encrypted using SSL. • UDP — Ports of this type apply only to connections that use the UDP protocol.
Categories	Classifies the function of the application; an application might be a member of multiple categories.
Capabilities	Displays sub-functions of the application; for some applications, certain sub-functions can be selectively disabled.
Risk	Rates the danger the application might pose to your organization.

Dependent applications

Dependent applications enable application-based allow rules to function as expected without creating an additional rule for each dependent application.

Some applications are dependent on other applications to function properly. When you create an Allow rule for an application, the rule might have to allow dependent applications. For example, a web application might have HTTP as a dependent application so content hosted on other sites still loads as expected.



Note: If the application allowed in a rule has a dependency on HTTP, some unknown HTTP traffic might also be allowed by the rule. This would only apply in the case where a later rule does not define HTTP.

Types of applications

There are three types of applications.

Related concepts

[Firewall applications](#) on page 168

[Custom applications](#) on page 170

Related reference

[Provided applications](#) on page 167

Provided applications

The firewall utilizes a database of application signatures that are pre-categorized and rated for risk.


Applications are created based on ongoing research. By default, your firewall is configured to download application updates daily to ensure the applications database remains up to date. You can view when the update

was last received on the **Dashboard**. You can configure update frequency and when the download takes place or update immediately in the **Updates** area. If your firewall is on isolated network, you can update the firewall applications manually.

Information about each application is available in the **Applications** area.

Some applications broadly classify connections while others are very specific. Refer to the table for examples.

Table 38: Application scope examples

Application	Matches
L2TP	All connections that use the Layer 2 Tunneling Protocol (L2TP)
TCP/UDP	All connections that use the TCP or UDP protocols
HTTP	All web-based applications (HTTP protocol on port 80 or SSL on port 443)
facebook	Only Facebook HTTP connections on TCP port 80 or 443 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Note: Other recognized web applications are not matched. </div>

When applications become obsolete or invalid, they are deprecated in the applications database. Deprecated applications cannot be selected when creating new rules or application groups.

When an application is deprecated, a message alerts you to the change.

Related tasks

[Updating application signatures on an isolated network](#) on page 177

Firewall applications

Firewall applications act as servers or clients.

They can perform either of the following functions:

- Process connections that are destined for the firewall
- Initiate connections on the firewall's behalf

Table 39: Firewall applications

Firewall application	Purpose
Active Passport*	Grants active passports to users.
Admin Console	Processes Sidewinder Admin Console connections from administrators.
BGP Routing Server	Participates in Border Gateway Protocol (BGP) routing.
Change Password Server	Allows external users to change their Sidewinder or LDAP password using a web browser.

Firewall application	Purpose
Cluster Registration Client*	Allows registration and communication among firewalls in High Availability (HA) clusters.
Cluster Registration Server*	Allows registration and communication among firewalls in High Availability (HA) clusters.
Common Access Card*	Allows administrators to log on to the firewall using a Common Access Card authenticator.
Control Center Status*	Communicates with Sidewinder Control Center if the firewall is managed by Control Center.
Control Center Management*	Communicates with Sidewinder Control Center if the firewall is managed by Control Center.
DHCP Relay	Forwards DHCP requests from clients to DHCP servers in different broadcast domains.
Enterprise Relay Server*	Allows services that need to communicate with each other in multi-firewall configurations.
ePolicy Orchestrator*	Allows communication between ePolicy Orchestrator and the firewall.
Trusted Source*	Sends Global Threat Intelligence queries to McAfee Global Threat Intelligence servers.
ISAKMP Server	Generates and exchanges keys for VPN sessions.
Login Console	Allows administrators log on at a console attached to the firewall.
McAfee Logon Collector*	Communicates with McAfee Logon Collector software that is installed on a Windows-based server.
Network Intelligence Manager*	Allows communication between McAfee EIA and the firewall.
OSPF IPv6 Routing Server	Participates in Open Shortest Path First IPv6 (OSPF IPv6) routing.
OSPF Routing Server	Participates in Open Shortest Path First (OSPF) routing.
Realtime Audit*	Allows the firewall to send audits in real time if the firewall is managed by Control Center.
RIP Routing Server	Participates in Routing Information Protocol (RIP) routing and learns routes without broadcasting routing information.
RIP Unbound Server	Participates in Routing Information Protocol (RIP) routing and automatically broadcasts routing information to all zones.
SecureAlert*	Communicates with Sidewinder Control Center if the firewall is managed by Control Center.
Sendmail Server	Processes email when hosted sendmail is enabled on the firewall.

Firewall application	Purpose
SmartFilter Admin Console	Communicates with the SmartFilter Administration Console.
SmartFilter Redirect Server*	Redirects web requests that are denied or coached by SmartFilter.
SNMP Agent	Communicates with SNMP management stations.
SSH Server	Accepts SSH connections from firewall administrators.
Telnet Server	Accepts Telnet connections from firewall administrators.
XORP PIMD	Participates in Protocol Independent Multicast - Sparse Mode (PIM-SM) routing.
You do not need to create access control rules for the firewall applications in the table that are marked with an asterisk (*).	

Custom applications

In addition to the provided applications and firewall applications, you can create custom applications.

A custom application combines the attributes of an existing parent application with new ports. Create a custom application when you want to override the ports of an application in the database.

The port types allowed for a custom application depend on the properties of the parent application. This example shows the ports you can specify for HTTP and NTP parent applications.

- **HTTP** — TCP and SSL ports because HTTP is a TCP protocol that can also use SSL.
- **NTP** — UDP ports because NTP uses the UDP protocol.

Application type scenario

Consider the applications listed in the table. All of the applications relate to SSH, but each application type matches SSH traffic that serves a slightly different purpose.

Table 40: Example SSH application types

Application name	Application type	Purpose
SSH	Provided	Matches SSH connections on port 22 that attempt to pass through the firewall
SSH-2022 [<i>user-specified name</i>]	Custom (dependent application is SSH)	Matches SSH connections on port 2022 that attempt to pass through the firewall
SSH Server	Firewall	Matches SSH connections that are destined to the firewall

Typical Scenarios

McAfee AppPrism can be applied to the firewall as a way to enforce your organization's policy.

To illustrate, this section discusses six typical scenarios and provides the high-level steps for each.

Use case - Selectively disable services

You can allow outbound HTTP traffic while disabling specific applications.

Assume you want to allow user access to the Internet but block users from uploading or downloading documents to Google Docs or Google Calendar. Google Docs Upload and Google Calendar are listed in the application signature database. Users can view and create Google documents using their web browser, but they cannot upload documents from their computer.

Use this type of policy to protect your network from outbound data loss and potential inbound malware.

Implementing this scenario involves these high level tasks:

- 1) Define the User group.
- 2) Create an access control rule that denies the applications, Google Docs Upload and Google Calendar.
- 3) Create an access control rule that allows HTTP.
- 4) Order your rules as needed.

Use case - Protecting company information

You can allow an inbound application while denying outbound traffic.

Assume you want users to be able to view and participate in WebEx conferences that are internal and external to your network, but you want to protect the user's screen from exposing potentially sensitive information to other attendees.

Use this type of policy to reduce the opportunity for unintended outbound data loss.

Implementing this scenario involves these high level tasks:

- 1) Define the User group.
- 2) Create an access control rule that denies WebEx desktop sharing.
- 3) Create an access control rule that allows HTTP.
- 4) Place the deny rule above the allow rule.

Use case - Limiting capabilities of allowed applications

You can allow an application to be used in the network while denying a specific capability of that application.

Assume you want users to be able to access Yahoo instant messaging, so that they can communicate with contacts outside the company, but you want to restrict the ability to send and receive files through this application.

Use this type of policy to protect your network from outbound data loss and inbound potential malware.

Implementing this scenario involves these high level tasks:

- 1) Define the User group.
- 2) Create an access control rule that allows Yahoo Messenger but disables the file sharing capability.
- 3) Order your rule as needed.

Use case - Blocking peer-to-peer access

You can deny specific categories of applications without needing to add new individual applications to the rule.

Assume you do not want users to participate in torrent sharing inside and outside your network. You can block the application category for all identified peer-to-peer applications, which will continue to expand as applications are added to the application signature database.

Use this type of policy to protect your network from outbound data loss, inbound potential malware, and pirating of copyrighted materials.

Implementing this scenario involves these high level tasks:

- 1) Define the User group.
- 2) Select the application category Peer to Peer (P2P), which includes all torrent applications.
- 3) Create an access control rule that denies or drops the application category.
- 4) Order your rule as needed.

Use case - Restricting streaming media

You can allow an application to be used in the network while blocking URL categories within that application.

Assume you want users to be able to access streaming media for web conferencing, but you want to restrict the types of media they can view. You can choose from a number of URL categories to block, such as those labeled as 'sports'.

Use this type of policy to protect your network from misappropriation of network resources, excessive bandwidth use, and potential malware.

Implementing this scenario involves these high level tasks:

- 1) Create or modify a SmartFilter URL filtering policy to block sports.

- 2) Create or modify an HTTP application defense that uses the SmartFilter policy.
- 3) Create or modify an application defense group that uses the HTTP application defense.
- 4) Create an access control rule that uses the application defense group defined above.
- 5) Order your rule as needed.

Use case - Enabling application discovery in SPAN mode

The firewall can passively listen to traffic while identifying applications.

Assume you want the firewall to inspect traffic without taking any action on it, but you want to know what applications are in use by your network. While configuring SPAN mode, you can enable **Application discovery** on the zone to make the firewall include application information in the data collected. We recommend having SSL decryption enabled for greater accuracy.

Use this type of policy to view applications in actual use by your network and assist in tailoring a policy to fit your organization.

Implementing this scenario involves these high level tasks:

- 1) Create a zone that has **Application discovery** enabled.
- 2) Create a SPAN interface.
- 3) Create a SPAN rule.
- 4) Order your rule as needed.

Manage applications




To manage applications, select **Policy > Rule Elements > Applications**. The **Applications** window appears.



Tip: For option descriptions, click **Help**.

Use the following instructions to view and create applications.

Table 41: Application management tasks

Task	Steps
Create a custom application	<ol style="list-style-type: none"> 1) Click New. 2) In the Applications: New Application window, complete the fields as appropriate. 3) Click OK, then save your changes.
Delete a custom application	<ol style="list-style-type: none"> 1) Select the application that you want to delete. 2) Click Delete. A confirmation pop-up window appears. 3) Click Yes, then save your changes.
Filter applications by category	<p>In the Filter by categories area, click one or more categories.</p> <p> Tip: To clear a category filter, click x on the category.</p>
Filter applications by risk	<p>In the Filter by risk area, click one or more risk buttons.</p> <p> Tip: To clear a risk filter, click the button again.</p>
Search applications	<p>Type your search criteria in the Search field.</p> <p> Tip: To clear your search, click x in the Search field.</p>
Rename a custom application	<ol style="list-style-type: none"> 1) Select the custom application that you want to rename. 2) Click Rename. 3) In the Applications: Rename window, type a new name for the custom application. 4) Click OK, then save your changes.
View audit data for an application	<ol style="list-style-type: none"> 1) Select the application that you want to view audit data for. 2) Click View Audit. The Applications: Audit Viewing window appears.
View where an application is used	<ol style="list-style-type: none"> 1) Select the application you want to investigate. 2) Click Usage. The Usage window appears.

Manage application groups

Application groups define common sets of applications that you want to reuse on multiple rules.

Steps


- 1) Select **Policy > Rule Elements > Applications**. The **Applications** window appears.
- 2) From the **Manage** drop-down list, select **Groups**. The **Application Groups** window appears.











Tip: For option descriptions, click **Help**.

Use the following instructions to manage application groups.

Table 42: Application group management tasks

Task	Steps
Add an application to an application group	<ol style="list-style-type: none"> 1) Select the application group to add the application to. 2) Add the application using one of the following methods: <ul style="list-style-type: none"> • Double-click the application in the Available list. • Select the application in the Available list, then click >>. <div style="margin-top: 10px;">  <p>Tip: To select multiple consecutive applications, press Shift key as you select the first and last applications. To select multiple non-consecutive applications, press the Ctrl key as you select each application.</p> </div> 3) Save your changes.
Create an application group	<ol style="list-style-type: none"> 1) Click New. 2) In the Name field, type a name for the application group. 3) In the Rule action area, select the type of rules the application group will be used in. <ul style="list-style-type: none"> • If you select Allow only, you might be able to disable some capabilities for the application group. • If you select Allow, Deny, or Drop, you cannot disable capabilities for the application group. 4) Add applications to the application group as appropriate. 5) Save your changes.

Task	Steps
Delete an application group	<ol style="list-style-type: none"> 1) Select the application group that you want to delete. 2) Click Delete. A confirmation pop-up window appears. 3) Click Yes, then save your changes.
Disable a capability	<ol style="list-style-type: none"> 1) Select the application group that you want to disable a capability for. 2) In the Capabilities list, deselect the capability you want to disable. <div style="margin-left: 20px;">  Tip: Capabilities that cannot be disabled are unavailable. </div> 3) Save your changes.
Filter available applications by category	<p>In the Filter by categories area, click one or more categories.</p> <div style="margin-left: 20px;">  Tip: To clear a filter, click x on the category. </div>
Filter available applications by risk	<p>In the Filter by risk area, click one or more risk buttons.</p> <div style="margin-left: 20px;">  Tip: To clear a filter, click the button again. </div>
Remove an application from an application group	<ol style="list-style-type: none"> 1) Select the application group to remove the application from. 2) Remove the application using one of the following methods: <ul style="list-style-type: none"> • Double-click the application in the Membership list. • Select the application in the Membership list, then click <<. <div style="margin-left: 20px;">  Tip: To select multiple consecutive applications, press Shift key as you select the first and last applications. To select multiple non-consecutive applications, press the Ctrl key as you select each application. </div> 3) Save your changes.
Rename an application group	<ol style="list-style-type: none"> 1) Select the application group that you want to rename. 2) Click Rename. 3) In the Rename window, type a new name for the application group. 4) Click OK, then save your changes.

Task	Steps
Search application groups	Type your search criteria in the application group area Search field.  Tip: To clear your search, click x in the Search field.
Search available applications	Type your search criteria in the Available area Search field.  Tip: To clear your search, click x in the Search field.
Search member applications	Type your search criteria in the Membership area Search field.  Tip: To clear your search, click x in the Search field.
View audit data for an application	Right-click the application that you want to view audit data for, then select View Audit . The Applications: Audit Viewing window appears.  Tip: To view audit data for multiple applications, press the Ctrl key as you select each application, then right-click a selected application and select View Audit .
View where an application group is used	<ol style="list-style-type: none"> 1) Select the application group you want to investigate. 2) Click Usage. The Usage window appears.
View where an application is used	Right-click the application you want to investigate, then select Usage . The Usage window appears.

Updating application signatures on an isolated network

For a firewall on an isolated network, you can update the AppPrism signatures manually.

Steps

- 1) Run the command to get the firewall serial number.

```
cf license query
```

- 2) Run the command to get the current version of the AppPrism database on the firewall.

```
cf appdb ver
```

- 3) Go to the firewall download page.

`http://sig.sidewinder.downloads.forcepoint.com/cgi-bin/appdb_update.py?serialNumber=<fw-serial-number>&downloadAPI=1.0&appdbVersion=<current-appdb-version>`

Where:

- `<fw-serial-number>` is the value of the `serial_number` field from step 1.
- `<current-appdb-version>` is the database version from step 2.

- 4) You will be prompted to save the latest signature file.

- 5) Transfer the file to a directory on the firewall, for example `/home/your_username`.

Transfer it using a CD-ROM:

- a) Burn the file to a CD-ROM.
- b) Insert the CD-ROM into the firewall.
- c) Run the following commands on the firewall:

```
mount_cd9660 -o ro /dev/acd0 /cdrom
cd /cdrom
cp applications.tar.enc /home/your_username
cd /
umount /cdrom
```

Transfer it using FTP:

- a) Place the file on an FTP server accessible by the firewall.
- b) Run the following commands on the firewall to retrieve the file:

```
cd /home/your_username
ftp ftpserver.domain.com (Enter login credentials)
cd destination/path
bin
get applications.tar.enc
quit
```

- 6) Install the AppPrism signature update by running this command

```
cf appdb install file=/home/your_username/applications.tar.enc
```

Result



Note: The firewall will not accept a signature package older than the one currently installed. Attempting to install an older signature package will result in an error audit.

Application Defenses

Contents

- [Understanding Application Defenses](#) on page 179
- [How the Generic Application Defense profile works](#) on page 182
- [Virus scanning](#) on page 186
- [Managing Application Defense groups](#) on page 188
- [Managing Application Defense profiles](#) on page 191

Application Defenses refine access control rules for specific applications that use proxies and filter agents.

Understanding Application Defenses

You can use Application Defenses to configure key services such as anti-virus, anti-spyware, and web services management.

Application Defense policy is configured with profiles and groups:

- **Application Defense profile** — Contains all the configuration options for the Application Defense. Multiple profiles can be created for each Application Defense.
- **Application Defense group** — Groups Application Defense profiles into a single object that is used by access control rules.

Application Defenses are applied to a connection when the connection matches an access control rule that contains both:

- An application rule element that includes a signature that corresponds to the Application Defense
- An Application Defense group that includes the Application Defense

Application Defense types

Most Application Defense types contain settings for a particular protocol or service. However, the Generic Application Defense contains settings that apply to the Application Defense group.

The Application Defense types are:

- **Citrix** — Configures advanced Independent Computing Architecture (ICA) proxy parameters.
- **FTP** — Configures File Transfer Protocol (FTP) permissions and file scanning for the FTP proxy.
- **Generic** — Configures connection settings, expected connection limits, traffic transparency, packet filtering, and stateful packet inspection. These settings apply to the Application Defense group that contains the Generic profile.
- **H.323** — Configures enforcement settings for H.323, a standard that provides support for audio and video conferencing across a shared medium such as the Internet.
- **HTTP** — Configures advanced parameters for HTTP or decrypted HTTPS and SSO access control rules.

- **IIOIP** — Configures enforcement settings for the IIOIP (Internet Inter-ORB Protocol) proxy, which makes it possible for distributed programs written in different programming languages to communicate over the Internet.
- **Mail (Sendmail)** — Configures advanced parameters for sendmail access control rules.
- **Mail (SMTP proxy)** — Configures filtering options for the SMTP proxy.
- **Oracle** — Configures continuous session monitoring to prevent spoofing and tunneling attacks while sessions are in progress for the SQL proxy.
- **SIP** — Configures media filtering, call duration, and peer types for the Session Initiation Protocol (SIP) proxy.
- **SNMP** — Configures advanced properties for the SNMP proxy.
- **SOCKS** — Configures advanced properties for the SOCKS proxy.
- **SSH** — Configures advanced properties for the SSH proxy.
- **T120** — Configures enforcements for the T.120 proxy. T.120 is a standard for real-time data conferencing.

Related concepts

[How the Generic Application Defense profile works](#) on page 182

Application Defense profiles

Application Defense profiles contain all the configuration options for the Application Defense.

Multiple profiles can be created for each Application Defense type. When configuring an Application Defense group, a profile is selected for each Application Defense.

Five Application Defense profiles are predefined:

- **Anti-Virus Scanning** — The Anti-Virus Scanning profile configures basic anti-virus scanning. Infected files will be discarded. This profile is provided for FTP, HTTP, and Mail (Sendmail) Application Defenses.
- **connection settings** — The connection settings profile provides timeout settings for connections. This profile is provided for the Generic Application Defense.
- **minimal proxy** — The minimal proxy profile forces all connections through a proxy. A minimal proxy Application Defense performs the least amount of content inspection possible. This profile is provided for all Application Defenses.
- **URL Filtering** — The URL Filtering profile uses SmartFilter for URL filtering. This profile is provided for the HTTP Application Defense.
- **URL Filtering and Anti-Virus Scanning** — The URL Filtering and Anti-Virus Scanning profile discards files infected with malware, and uses SmartFilter for URL filtering. This profile is provided for the HTTP Application Defense.

Application Defense groups

Each access control rule uses an Application Defense group to specify advanced application policy.

When you create an Application Defense group, you can select a single profile for each Application Defense type to populate the Application Defense group.

- Each Application Defense group must contain a Generic Application Defense profile. The Generic Application Defense controls connection settings for all protocols, and is the only Application Defense required in every Application Defense group.

- All other Application Defense profiles are optional.
If the access control rule allows an application and you do not specify a corresponding Application Defense profile, no Application Defense settings are applied to that application.
- The Application Defense profiles in the group do not need to match the applications used on the access control rule.
If the group contains an Application Defense profile for an application that is not used by the access control rule, the profile settings are ignored by the rule.



Note: If the access control rule that matches the SSL connection specifies an Application Defense group that does not assign an HTTP Application Defense (for example, the connections settings group initially specified as the <Default Group>), the following SSL rule Decrypt/Re-encrypt selections are not enforced: **Display notification to web browser** and **Perform certificate hostname matching**.

How Application Defense groups affect connection processing

The Application Defense group you associate with an access control rule affects how the firewall processes matching connections.

By default, the firewall uses IP filters to pass matching connections unless the protocol or other policy configuration requires a proxy. If the Application Defense group contains enforcements that require proxies, such as virus scanning or SmartFilter, the firewall automatically uses proxies as needed. A proxy is also required when using Global Threat Intelligence or a domain network object in an access control rule.

You can configure the firewall to use a proxy for a specific application by:

- Selecting an Application Defense profile for that application in the Application Defense group
- Enabling the following options on the Generic Application Defense profile:
 - Use TCP proxy
 - Use UDP proxy
 - Use ICMP proxy

Related concepts

[Configuring packet filters](#) on page 184

Default Application Defense group

You set one Application Defense group as the default. The default Application Defense group is used in all new access control rules that use an Application Defense group, unless you select a different Application Defense group for the new rule in the **Rules** window.

For example, a more restrictive Application Defense group can be created for emergency situations. When a real-time threat is discovered, this more restrictive Application Defense group can be made the default, saving administrators from having to edit every rule. After the situation is resolved, the previous default Application Defense group can be restored.

Predefined Application Defense groups

Five Application Defense groups are already defined.

- **Anti-Virus Scanning** — The **Anti-Virus Scanning** Application Defense group assigns the **Anti-Virus Scanning** Application profile to the FTP, HTTP, and Mail (Sendmail) Application Defenses. All other Application Defenses are set to the **minimal proxy** profile. Use this Application Defense group in an access control rule to enable anti-virus scanning.
- **connection settings** — The **connection settings** Application Defense group contains only the connection settings profile for the **Generic** Application Defense. All other Application Defenses are set to **<None>**. When this Application Defense group is included in an access control rule, no content inspection will be performed; packet filters will be used instead. Use the **connection settings** Application Defense group when no enforcement is necessary.
- **minimal proxy** — The **minimal proxy** Application Defense group includes the **minimal proxy** profile for every Application Defense. Use the **minimal proxy** Application Defense group in an access control rule when only minimal enforcement is necessary.
- **URL Filtering** — The **URL Filtering** Application Defense group assigns the **URL Filtering** profile to the HTTP Application Defense. All other Application Defenses are set to the **minimal proxy** profile. Use this Application Defense group in an access control rule to enable URL Filtering.
- **URL Filtering and Anti-Virus Scanning** — The **URL Filtering and Anti-Virus Scanning** Application Defense group assigns the **URL Filtering and Anti-Virus Scanning** profile to the HTTP Application Defense, and assigns the **Anti-Virus Scanning** profile to the Mail (Sendmail) Application Defense. All other Application Defenses are set to the **minimal proxy** profile. Use this Application Defense group in an access control rule to enable URL filtering and anti-virus scanning.



Note: During an upgrade from 7.x, the predefined Application Defense profiles and groups are not created and do not appear for the firewalls that are upgraded.

How the Generic Application Defense profile works

The Generic Application Defense profile contains settings that apply to the Application Defense group. Access control rules that use the Application Defense group inherit the Generic Application Defense profile settings.

You can use the Generic profile to:

- **Set expected connections** — Configure the maximum number of connections for each agent.



Note: These settings affect the entire firewall and are not tied to a particular profile.

- **Force the use of proxies** — Select one or more of the checkboxes to force applications to run through the selected proxies.
- **Set timeouts** — Set the length of time, in seconds, that the firewall will wait before closing a connection.
 - **TCP connection timeout** — Set the length of time, in seconds, that is allowed for the TCP connection to establish. Valid values are 1—65535.
 - **TCP idle timeout** — Set the length of time, in seconds, that the TCP connection can remain idle before it is closed. Valid values are 0—2147483647. A value of 0 means the session will never time out.
 - **UDP idle timeout** — Set the length of time, in seconds, that the UDP session can remain idle before it is closed. Valid values are 0—2147483647. A value of 0 means the session will never time out.

- **(ICMP Packet Filter only) Response timeout** — Set the length of time, in seconds, that a session will await responses after the final request. Valid values are 1—100000.
- **Configure transparency settings** — Enable or disable support for non-transparent connections by proxy agent.
- **Configure stateful inspection** — Configure stateful packet inspection properties, and to select the response types you want to allow for an access control rule.
- **Configure IPv6 extension header filtering** — Configure which IPv6 extension headers and options are allowed through the firewall. By default, IPv6 extension headers are not allowed.
- **Configure IP filter settings** — Configure advanced settings for IP filters, including request rate and auditing parameters.

Expected Connections

Certain proxy agents can be configured to enable multiple instances of the same agent in order to load the traffic across the multiple instances.

Multiple instantiation of proxy agents is useful for hardware configurations with multiple CPUs or sites that have experienced problems due to an exceedingly large amount of concurrent connections through one of those proxies.

A single proxy instance for any of these agents can generally handle up to 2000 sessions (a session consists of two connections for most protocols). By default, most proxy agents are configured for 4 proxy instances, or about 8000 sessions. This quantity is more than adequate for most sites. However, if your site is consistently recording concurrent sessions that hover around the 8000 range (or if you have experienced problems because the number of connection attempts is significantly higher) for any of these proxies, you might need to increase an agent's number of expected connections in order to enable additional instances for that proxy agent.

The following proxy agents support multiple instantiation:

- Citrix Proxy agent
- FTP Proxy agent
- HTTP Proxy agent
- MS-SQL Proxy agent
- Oracle Proxy agent
- SMTP (Mail) Proxy agent
- SOCKS Proxy agent
- SSH Proxy agent.

The default value for all agents is 8000 connections. You can specify expected connection values from 1000–32000.

Passing traffic transparently and non-transparently

On the Sidewinder, FTP, HTTP, Oracle, and Telnet applications can be configured to be *transparent* or *non-transparent*.

For transparent connections, the client is unaware of the firewall. The firewall is implicitly included in the path based on routing. For non-transparent, the client is aware of the firewall and explicitly connects to the firewall. The connection type is determined on the client side (browser settings or user entering the firewall IP address).

Proxy agents can be configured to allow only transparent connections, only non-transparent connections, or both, depending on which option is indicated in the **Generic Application Defense: Connection Settings** window.

When using transparent settings, the user appears to connect directly to the desired network server without connecting to the firewall first. For example, to initiate an outbound Telnet session using a transparent Telnet proxy agent, a user would issue the following command from his or her computer and then connect directly to the external Telnet server:

```
telnet destination
```

With a non-transparent Telnet proxy agent, a user must first Telnet to the firewall and specify a destination for the Telnet session. For example, the following shows how an internal user would initiate a Telnet session to a server in an external network using a non-transparent proxy that requires standard password authentication.

```
telnet firewall_IP_address
```

(connection message from the firewall appears...)

```
Enter destination: destination_IP_address
```

(authentication prompt from the firewall appears...)

```
Username: username
```

```
Password: password
```

(connection message from the destination Telnet server appears...)

```
login: username
```

Non-transparent proxy configurations are typically used in networks that use NAT. For example, you would use a non-transparent agent if your end users need to access a non-standard port or if there is no direct route between the client and the intended server.



Note: Certain transparent and non-transparent proxy configurations can require users to authenticate before they are allowed to connect.

Allowing non-transparent traffic requires configuring end-user browsers to point to the firewall. To set up browsers to work with the non-transparent proxy option, there are two basic steps:

- Specify the firewall fully qualified host name or IP address in the browser proxy line.
- Specify the port number for the proxy agent.



Note: If you want users connecting to port 80 to be able to pass HTTPS traffic through the firewall, make sure port 80 is specified in the **Destination ports allowed through non-transparent HTTP** proxyfield on the **HTTP Application Defense: Connection** tab.

Consult your browser documentation for defining an HTTP proxy server.

Configuring packet filters

If you do not want to do any content inspection on particular traffic, you might want to pass traffic using a packet filter, also called an IP filter.

Packet filters will examine the following attributes of a connection:

- Source IP address
- Destination IP address
- Protocol
- Source port

- Destination port
- [Optional] Connection state
- [FTP only] Data channel negotiation

Packet filters support these rule configurations:

- Zone matching
- NAT and redirect
- Passive Passport
- IPS inspection

There are three *Use proxy* options available — **Use TCP proxy**, **Use UDP proxy**, and **Use ICMP proxy**. These options are in the Generic application defense and can be used to specify whether the connection should use a proxy or packet filter.



Note: Certain applications, such as those that require proxy settings, will always use a proxy regardless of how the *Use proxy* settings are configured. Traffic matching a rule that uses Global Threat Intelligence or a domain network object will always be handled by a proxy.

Use these high-level steps to make sure that your traffic uses a packet filter:

- 1) Create a new **TCP/UDP** application and specify the ports as needed.
- 2) Create or use a Generic Application Defense that does not have the *Use proxy* settings enabled.
- 3) Create or use an Application Defense group that references the Generic Application Defense you created in the previous step. Configure only the Generic Application Defense and set the other Application Defenses to **<None>**.
- 4) Create a rule that uses your custom application and the packet filter Application Defense group.

Related concepts

[How Application Defense groups affect connection processing](#) on page 181

Stateful packet inspection

The firewall can actively track IP-based sessions using *stateful inspection*.

Stateful inspection ensures that only packets valid for a new session or a portion of an existing session are sent on to the final destination.

How traffic is filtered if stateful packet inspection is enabled

When the firewall receives IP-based traffic, it starts by checking a filter session record database to determine if an active session record exists for this traffic.

A session record indicates that this traffic is in response to a previous successful match to an allow rule. Session records only exist if the matching access control rule had stateful packet inspection enabled.

- **If an active session record exists**, the following occurs:
 - Perform address and port rewriting, if required
 - Perform session processing
 - Forward packet directly to the correct destination interface without any additional processing
- **If no active session record exists**, the firewall checks the active access control rules to find a match.
 - If a matching allow rule does exist, the packets are processed according to the rule.
 - If no matching access control rule exists, the packet is generally denied. Exceptions:
 - If the packet arrived on a zone that is configured to hide port unreachables, the packet is dropped instead of denied.
 - If an application is listening on the packet port, the application handles the packet according to its protocol standards.

How traffic is filtered if stateful packet inspection is disabled

When the firewall receives traffic, it checks the active access control rules for a matching rule.

The firewall then does one of the following:

- If an access control rule match is found, the packet source or destination address are translated according to the translation information that is configured for that rule. The packet is then forwarded on for any further firewall processing.
- If there are no matching access control rules in the filter database, the firewall sends the packet on to application-layer processing.

Understanding stateful session failover in an HA cluster

When filter session sharing is configured for an HA cluster, the processing firewall sends out multicast messages over the heartbeat interface to notify the other node of packet filter session activity (such as a new session, closed session, or change in session state).

Each time a node receives a message, it updates its local session table accordingly. All sessions received from the primary will have a status of shared on the secondary/standby.

When HA causes a secondary/standby to take over as the acting primary, the shared sessions on the acting primary become available. When a packet is received for a session, it will be validated against the rules of the processing node. The processing node will then begin sending multicast state-change messages.

Virus scanning

Virus scanning is supported for some Application Defense profile types.

- HTTP
- FTP
- Mail (Sendmail)

Virus scanning is configured by defining virus/spyware rules. By default, a single allow rule is contained in the filter rule table. If you choose to leave the default allow rule as the last rule in your table (that is, all traffic that isn't explicitly denied will be allowed), you will need to configure the appropriate virus/spyware scan and/or deny rules and place them in front of the default allow rule. If you configure the default rule action to deny (that is, all traffic that is not explicitly allowed will be denied) you will need to configure the appropriate *virus/spyware scan and/or allow* rules and place them in front of the default deny rule.



Note: Filtering rules that are configured with an allow or deny action will allow or deny traffic based on the rule criteria that is defined for those rules. Allow and deny rules do not perform virus and spyware scanning. To perform virus and spyware scanning for traffic that matches a rule before it is allowed, you must specify **Anti-Virus Scanning** in the rule's **Application Defense** field.

Create a virus/spyware rule

Create a virus/spyware rule to enable scanning for a particular file type.

Steps

- 1) Select **Policy > Application Defenses**.
- 2) Select the HTTP, FTP, or Mail (Sendmail) Application Defense profile you want to configure virus scanning for, then click the appropriate tab:
 - **FTP** — Click the **Virus/Spyware** tab.
 - **HTTP or Mail (Sendmail)** — Click the **MIME/Virus/Spyware** tab.
- 3) Click **New**. The **Rule Edit** window appears.



Tip: For option descriptions, click **Help**.

- 4) Configure the rule as appropriate, then click **OK**.
- 5) Save your changes.

Configure the default filtering action

The default filter rule is a general rule designed to occupy the last position in your rule table.

To configure the default action:

Steps

- 1) Select **Policy > Application Defenses > Defenses**.
- 2) Select the HTTP, FTP, or Mail (Sendmail) Application Defense profile you want to configure virus scanning for, then click the appropriate tab:
 - **FTP** — Click the **Virus/Spyware** tab.
 - **HTTP or Mail (Sendmail)** — Click the **MIME/Virus/Spyware** tab.

- 3) Select the default rule in the table, then and click **Modify**. The **Default Action** window appears.



Tip: For option descriptions, click **Help**.

- 4) Select the appropriate action for this rule.
 - **Allow** — The default rule is initially configured to *allow* all data that does not match other filter rules. If you leave the default rule as an allow rule, you must create filter rules that require virus scanning or explicitly deny any extensions that you do not want to allow, and place them in front of the default allow rule.
 - **Deny** — If you prefer the default rule to *deny* all data that did not match a filter rule, you must create the appropriate virus scan and allow rules and place them in front of the default deny rule.
 - **Virus/Spyware Scan** — If you want to perform virus and spyware scanning for traffic that does not match any allow or deny filter rules you create, select this option. You will then need to create the appropriate allow and deny rules that will not require scanning.
- 5) Click **OK**, then save your changes.

Managing Application Defense groups

To manage an Application Defense group, select **Policy > Application Defenses > Groups**. The **Application Defense groups** window appears.

- The upper pane lists all of the Application Defense groups that are currently configured. Columns show which profile is selected for each Application Defense. The Application Defense group in bold is set as the default Application Defense group for all new rules.
- The lower pane lists each Application Defense in the left column. When you select an Application Defense in the table, the available profiles can be selected from the drop-down list in the right column.

Create an Application Defense group

Create a new Application Defense group if you want to use a new set of Application Defense profiles in one or more access control rules.

Steps


- 1) Select **Policy > Application Defenses > Groups**.
- 2) In the upper pane, click **New**. The **New Groups Application Defense** window appears.




Tip: For option descriptions, click **Help**.

- 3) Type a name for the Application Defense group, then click **OK**. The Application Defense group appears in the list in the upper pane.
- 4) In the lower pane, type a description for the Application Defense group.

- 5) In the lower pane, configure which Application Defense profiles belong to this group.
 - a) Select or configure a **Generic** Application Defense profile to provide settings for the group.

 **Note:** You must select a **Generic** Application Defense profile. The other Application Defense profiles are optional.
 - b) [Optional] For each application you want to apply Application Defense settings to, select or create an Application Defense profile.


 **Note:** To allow FTP over IPv6, make sure **<None>** is selected for FTP.
- 6) Click **OK**. The selections in the **Name** column appear in the corresponding columns in the upper pane.
- 7) Save your changes.


Modify an Application Defense group

Modify an Application Defense group to change the Application Defense profiles that are already in use.

Steps

- 1) In the upper pane, select the appropriate Application Defense group.

 **Tip:** For option descriptions, click **Help**.
- 2) In the lower pane, make the appropriate changes.


 **Tip:** To make your changes in a pop-up window, select the Application Defense group and then click **Modify**.
- 3) Save your changes.

Rename an Application Defense group

Renaming an Application Defense group does not affect how the group is used.

Steps

- 1) In the upper pane, select the appropriate Application Defense group.

 **Tip:** For option descriptions, click **Help**.
- 2) Click **Rename**.
- 3) Type a new name in the pop-up window, then click **OK**.

- 4) Save your changes.

Delete an Application Defense group

Delete an Application Defense group if it is no longer used.

Steps

- 1) In the upper pane, select the appropriate Application Defense group.



Tip: For option descriptions, click **Help**.

- 2) Click **Delete**.
- 3) Confirm deletion in the pop-up window, then save your changes.

Make a group the default Application Defense group

The default Application Defense group is used in every access control rule that uses the <Default> Application Defense, unless you select a different Application Defense group in the **Rules** window.

In the upper pane, select the appropriate Application Defense group, then click **Set Default**.

View which access control rules are using an Application Defense group

View where an Application Defense group is used to determine how the settings are applied in your policy.

Steps

- 1) In the upper pane, select the appropriate Application Defense group.



Tip: For option descriptions, click **Help**.

- 2) Click **Usage**. A pop-up window appears listing the access control rules that are currently using the selected Application Defense group.
- 3) When you are finished, click **Close**.

Duplicate an Application Defense group

Duplicate an Application Defense group if you want to use an existing group as the basis for a new group.

Steps

- 1) In the upper pane, select the appropriate Application Defense group.



Tip: For option descriptions, click **Help**.

- 2) Click **Duplicate**.
- 3) In the pop-up window, type a name for the duplicated Application Defense group, then click **OK**.
- 4) Make the appropriate modifications to the duplicated Application Defense group.
- 5) Save your changes.

Create or modify an Application Defense profile

Create or modify an Application Defense profile if the existing profiles don't meet the needs of the group.

Steps

- 1) In the upper pane, select the appropriate Application Defense group.
- 2) In the lower pane, click **New** or **Modify**.



Tip: For option descriptions, click **Help**.

- 3) In the pop-up window, configure the Application Defense profile.
- 4) When you are finished, click **OK**, then save your changes.

Managing Application Defense profiles

To view the Application Defense windows, select **Policy > Application Defenses > Defenses**, and then select the Application Defense you want to view from the tree.

The top pane of each Application Defense window consists of a table that lists all of the profiles (by row) that are currently configured for the Application Defense category selected in the tree.

- The profiles that are displayed in the table will vary depending on the Application Defense category you select from the tree.

- The table columns display the attributes for the selected Application Defense profile. The columns will vary by Application Defense.
- Basic default profiles, such as minimal proxy, are pre-configured for each Application Defense.

You can perform these actions in an Application Defense window:

Create a new Application Defense profile

Create an Application Defense profile to define a custom set of enforcements that can be reused in multiple Application Defense groups.

Steps

- 1) Select **Policy > Application Defenses > Defenses**.
- 2) Select the appropriate type of defense in the tree, then click **New**. The **New Application Defense** window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for your profile. If you are creating an HTTP Application Defense profile, select a type.
- 4) Click **OK**.
- 5) Modify the properties in the lower portion of the window, then save your changes.

Duplicate an existing Application Defense profile

Duplicate an Application Defense profile if you want to use an existing profile as the basis for a new profile.

Steps

- 1) Select the appropriate profile from the table, then click **Duplicate**. The **New/Duplicate Application Defense** window appears.



Tip: For option descriptions, click **Help**.

- 2) Type a name for your profile.



Note: If you are duplicating an HTTP Application Defense profile, you cannot select a type.

- 3) Click **OK**.
- 4) Modify the properties in the lower portion of the window, then save your changes.

Modify an existing Application Defense profile

Modify an existing profile if you want to change the settings used in your policy.

Steps

- 1) Select the profile that you want to modify from the table.



Tip: For option descriptions, click **Help**.

- 2) Modify the configuration information in the bottom portion of the window.



Tip: To modify the profile in a pop-up window, click **Modify**.

- 3) When you are finished, save your changes.

Rename an existing Application Defense profile

Renaming an Application Defense profile does not affect how the profile is used.

Steps

- 1) Select the appropriate profile from the table, then click **Rename**.



Tip: For option descriptions, click **Help**.

- 2) Type a new name in the pop-up window.

- 3) Save your changes.

Delete an existing Application Defense profile

Delete an Application Defense profile if it is no longer used. You cannot delete an Application Defense profile if it is being used in an Application Defense group.

If the profile is used in an Application Defense group, a pop-up window appears informing you which Application Defense groups are currently using this Application Defense profile.

Steps

- 1) Select the appropriate profile from the table, then click **Delete**.



Tip: For option descriptions, click **Help**.

- 2) In the pop-up window, confirm the deletion.

- 3) Save your changes.

View the Application Defense groups in which an Application Defense profile is used

View where an Application Defense profile is used to determine how the settings are applied in your policy.

Steps

- 1) Select the appropriate profile, then click **Usage**.



Tip: For option descriptions, click **Help**.

- 2) A pop-up window appears listing the Application Defense groups that are currently using the specified profile.
- 3) When you are finished, click **Close**.

[Generic only] Configure Expected Connections

Certain proxy agents can be configured to enable multiple instances of the same agent in order to load the traffic across the multiple instances.

If your site consistently records concurrent sessions that hover around the 8000 range, or if you have experienced problems because the number of connection attempts is significantly higher, you might need to increase an agent's number of expected connections in order to enable additional instances for that proxy agent.

Steps

- 1) Click **Set Expected Connections**.



Tip: For option descriptions, click **Help**.

The **Application Defenses: Expected Connections** window appears.



Tip: Specify the total number of connections expected for agents that support multiple instances, then click **OK**.

- 2) Save your changes.

Related concepts

[Expected Connections](#) on page 183

[HTTP only] Configure URL translation rules

Use URL translation to configure your firewall to redirect inbound HTTP connections based on the URL contained in the HTTP request.

By examining the HTTP application layer data, the firewall determines which internal web server inbound requests are destined for even if multiple servers share the same external IP address, as is common in virtual hosting environments.

Steps

- 1) Click **URL Translation Rules**. The **Application Defenses: URL Translation Rules** window appears.



Tip: For option descriptions, click **Help**.

- 2) Create URL translation rules as needed.
- 3) When you are finished, click **OK**, then save your changes.

Related tasks

[Create a URL translation rule](#) on page 229

[Mail (Sendmail) only] Configure sendmail properties

Use the Sendmail Properties window to edit sendmail configuration files.

Steps

- 1) Click **Sendmail Properties**. The **Application Defenses: Sendmail Properties** window appears.



Tip: For option descriptions, click **Help**.

- 2) Configure sendmail properties as appropriate, then click **OK**.
- 3) Save your changes.

Related concepts

[Editing sendmail files on Sidewinder](#) on page 498

[SSH only] Configure SSH known hosts

Manage SSH known hosts and server keys if your firewall is configured to decrypt and inspect SSH content.

Steps

- 1) Click **SSH Known Hosts**. The **Application Defenses: SSH Proxy Agent Properties** window opens.



Tip: For option descriptions, click **Help**.

- 2) Manage SSH known hosts and server keys as appropriate.
- 3) When you are finished, click **OK**, then save your changes.

Related tasks

[Create or modify an SSH known host key](#) on page 256

Access control rules

Contents

- [Creating and managing access control rules](#) on page 197
- [Configuring access control rules](#) on page 197
- [Examine how access control rules overlap](#) on page 204
- [Create access control rules and groups](#) on page 207
- [Modify access control rules and groups](#) on page 208
- [Arrange access control rules and groups](#) on page 208
- [View access control rules and groups](#) on page 209
- [Modify general settings](#) on page 211

Access control rules enforce policy on the firewall.

- Connections that match an access control rule are processed according to that rule.
- Connections that do not match an access control rule are denied.

Review the related topics in the *Policy overview* and *Policy in action* chapters to learn more about access control rule concepts and scenarios for applying them.

Creating and managing access control rules

This chapter explains how to create and manage access control rules. Review the related topics in the *Policy overview* and *Policy in action* chapters to learn more about access control rule concepts and scenarios for applying them.

Related tasks

- [Create or modify a zone](#) on page 370
- [Create or modify a zone group](#) on page 371
- [Delete a zone or zone group](#) on page 372
- [Create an access control rule](#) on page 203

Configuring access control rules

When configuring access control rules, determine what you want the firewall to do with different types of connections.

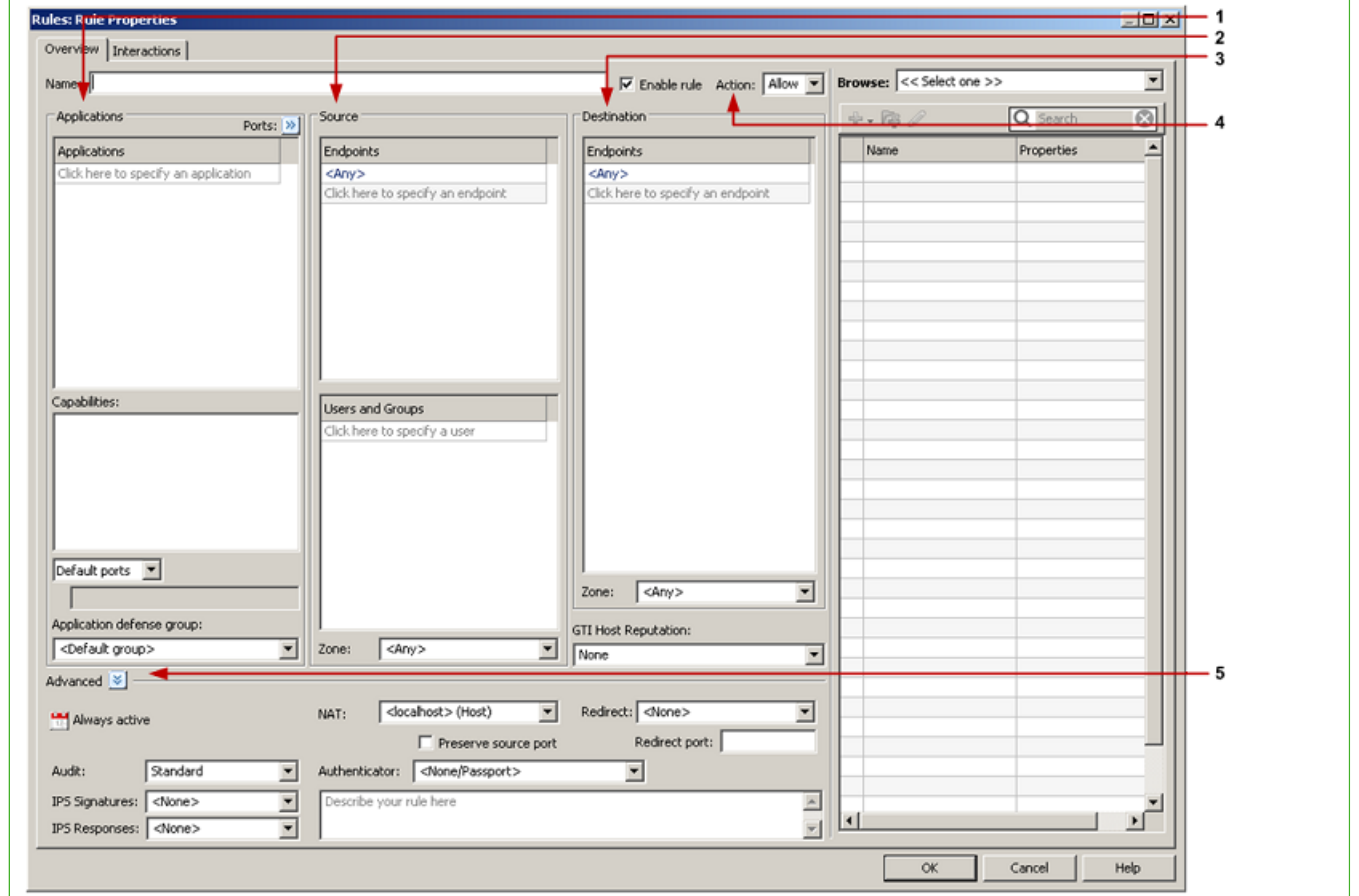
Ask these main questions:

- What connections should the rule match?
- What action should the firewall take on connections that match the rule?

These questions dictate the workflow you must follow to create a new access control rule. The following table shows this workflow.

To configure access control rules, select **Policy > Access Control Rules**.

Figure 32: Workflow to create an access control rule



- 1) Applications
- 2) Source
- 3) Destination
- 4) Action
- 5) Advanced options

For example, assume that you want to allow all members of the HR group in the internal zone to browse the Internet. The following table contains the elements that you must specify on an access control rule to accomplish this goal.



Note: To select the HR group, this scenario assumes that the firewall is configured to retrieve user information from McAfee Logon Collector software installed on a Windows server in the network.

Table 43: Required elements

Element	Configuration
Action	Allow
Applications	HTTP
Source Endpoints	<Any>
Source Users and Groups	HR
Source Zone	internal
Destination Endpoints	<Any>
Destination Zone	external

In this scenario, you would create an access control rule based on the elements shown in the table:

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rules: Rule Properties** window appears.
- 3) In the **Name** field, type a name for the access control rule, such as `HR_HTTP`.
- 4) From the **Action** drop-down list, select **Allow**.
- 5) In the **Applications** pane, select **HTTP**.
- 6) In the **Source** area, specify the connection sources to match.
 - a) In the **Endpoints** pane, verify that **<Any>** is specified.
 - b) In the **Users and Groups** pane, select the **HR** group.
 - c) From the **Zone** drop-down list, select **internal**.
- 7) In the **Destination** area, specify the connection destinations to match.
 - a) In the **Endpoints** pane, verify that **<Any>** is specified.
 - b) From the **Zone** drop-down list, select **external**.
- 8) Click **OK**, then save your changes.

Configuring access control rule attributes

Access control rules are made up of condition and action elements. Some elements are required for all access control rules, while the optional elements allow you to tailor rules to meet your specific needs.

Related concepts

[Required elements for access control rules](#) on page 200

[Optional condition elements for access control rules](#) on page 200

Related reference

[Optional action elements for access control rules](#) on page 202

Required elements for access control rules

Three elements are required when configuring an access control rule.

- **Name**
- **Applications** (Specify at least one application)
- **Action**

Optional condition elements for access control rules

The condition elements in the following table are optional. You can configure any of these elements as appropriate to restrict which connections match the access control rule.

Table 44: Optional condition elements

Optional element	Default configuration	Result of default configuration
Application Capabilities	Enabled	All capabilities of the selected applications match.
<i>Application ports</i>	Default ports	The default ports for the selected applications match.
Source Endpoints	<Any>	All endpoints in the selected source zones match.
Source Users and Groups	None specified	User identity is not used to match connection sources.
Source Zone	<Any>	All selected source endpoints match regardless of which zone contains them.
Destination Endpoints	<Any>	All endpoints in the selected destination zones match.

Optional element	Default configuration	Result of default configuration
Destination Zone	<Any>	All selected destination endpoints match regardless of which zone contains them.
GTI Host Reputation	None	The Global Threat Intelligence reputation scores of endpoints are not used to perform matching.

Disable application capabilities

Some applications include sub-functions, or capabilities, which can be selectively disabled. When capabilities are disabled, they do not match the access control rule.

Steps

1) Select **Policy > Access Control Rules**.

2) Open the rule you want to modify.



Tip: For option descriptions, click **Help**.

3) To disable capabilities for the access control rule, deselect them in the **Capabilities** field. When you disable a capability, it is disabled for all selected applications.



Note: You cannot disable a capability if it is required by any of the selected applications.

Override application ports

The default application ports can be overridden on access control rules. If you override the default ports, the custom ports apply to all appropriate selected applications.

Steps

1) Select **Policy > Access Control Rules**.

2) Open the access control rule you want to modify.



Tip: For option descriptions, click **Help**.

3) From the ports drop-down list, select **Override ports**.

4) In the text field, modify the ports.

- Prefix ports with the appropriate type (example: TCP/*n*, SSL/*n*, or UDP/*n*).
- Use commas to separate multiple ports of the same type (example: SSL/443,5190).
- Use spaces to separate different port types (example: TCP/80 SSL/443).

- Use a dash to create port ranges (example: TCP/8100-8200).

Note that:

- The custom TCP ports apply to both SMTP and HTTP because both applications allow TCP ports.
- The SSL ports apply only to HTTP because the SMTP application does not allow SSL ports.

Optional action elements for access control rules

The action elements in the following table are optional. You can configure any of these elements as appropriate to enable additional connection processing options.

By default, the optional action elements are hidden in the **Advanced** pane. To show or hide the **Advanced** pane, click the button next to **Advanced**.

Table 45: Optional action elements

Optional element	Default configuration	Result of default configuration
NAT	<localhost>	When matching connections leave the firewall, the source IP address is replaced with the firewall's IP address in the destination zone.
Redirect	<None>	Redirection is not performed for matching connections.
<i>Time Period</i> [calendar icon]	Always active	The access control rule is always active.
Audit	Standard	Major errors and informational messages are recorded.
IPS Signatures	<None>	IPS inspection is not performed for matching connections.
IPS Responses	<None>	IPS inspection is not performed for matching connections.
Authenticator	<None/Passport>	Passport is used to validate user identity instead of an authenticator.
Application defense group	<Default group>	The Application Defense group that is configured as the default is used.

Select elements using the browse pane for access control rules

The browse pane is a multi-function browser that allows you to modify and select various elements.

- Applications
- Application Defense group
- Endpoints

- **Users and Groups**
- **NAT**
- **Redirect**
- **Zones**

The browse pane is context-sensitive; different options are displayed based on the field you are browsing. Select the field you want to browse in either of the following ways:

- Click inside the appropriate field.
- From the **Browse** drop-down list, select the appropriate area.

For example, perform the following steps to select elements for the **Source Endpoints** field.

Steps

1) Select **Policy > Access Control Rules**.

2) Open the access control rule you want to modify.



Tip: For option descriptions, click **Help**.

3) Select the field using one of the following methods:

- Click inside the **[Source] Endpoints** pane.
- From the **Browse** drop-down list, select **Source endpoints**.

The browse pane switches to the **Source endpoints** view.

4) In the browse pane, you can:

- Select an object by selecting the corresponding checkbox.
- Add, modify, and search objects using the toolbar.

Create an access control rule

Create and configure an access control rule.

Steps

1) Select **Policy > Access Control Rules**.

2) Click **New > New Rule**. The **Rules: Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

3) In the **Name** field, type a name for the access control rule.

- 4) Specify applications to match.
 - Select applications in the **Applications** pane.
 - Enable or disable application capabilities in the **Capabilities** pane.
 - Specify advanced application settings by selecting an Application Defense group.
- 5) Select the sources to match.
 - Select endpoints in the **[Source] Endpoints** pane.
 - Select users and groups in the **[Source] Users and Groups** pane.
 - Select zones and zone groups from the **[Source] Zones** drop-down list.
- 6) Select the destinations to match.
 - Select endpoints in the **[Destination] Endpoints** pane.
 - Select zones and zone groups from the **[Destination] Zones** drop-down list.
 - Select the Global Threat Intelligence reputation scores to match.
- 7) Select an action.
 - **Allow**
 - **Deny**
 - **Drop**



Tip: A deny rule notifies the sender that the request was rejected while a drop rule does not.

- 8) [Optional] Enable connection processing options.
 - **NAT**
 - **Redirect**
 - **Audit**
 - **IPS**
- 9) Click **OK**, then save your changes.

Related tasks

[Create access control rules and groups](#) on page 207

Examine how access control rules overlap

Access control rules can potentially overlap in multiple ways. When rules overlap, they can interact to create unintended results that can be difficult to troubleshoot.

For example, consider two outbound access control rules that share the same condition elements except for overlapping source endpoints.

Table 46: Example intersecting access control rules

Rule name	Position	Source endpoint	Intersection of source endpoints
HTTP_1	n	1.1.1.20-1.1.1.60	1.1.1.40-1.1.1.60
HTTP_2	n+1	1.1.1.40-1.1.1.80	

In this example, hosts with IP addresses inside the intersection of source endpoints always match access control rule HTTP_1, even though it looks like they should match HTTP_2.

To view interaction information for an access control rule:

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Open the access control rule you want to examine.



Tip: For option descriptions, click **Help**.

3) Click the **Interactions** tab.

Note: To view the **Interactions** tab, the **Name** and **Applications** fields must be configured.

Figure 33: Interactions tab (Rule Properties window)

Position	Name	Action	Application	Ports	Source	Users	Source Zone	Destination
1	Internet Services	Allow	FTP, HTTP, ICMP,...	TCP/21, 80, 554,...	<Any>	<None>	internal	<Any>
3	HTTP_1	Allow	HTTP	TCP/80 SSL/443	Range 1 (IP Range)	<None>	internal	<Any>
4	HTTP_2	Allow	HTTP	TCP/80 SSL/443	Range 2 (IP Range)	<None>	internal	<Any>
5	Copy of HTTP_1	Allow	HTTP	TCP/80 SSL/443	Range 1 (IP Range)	<None>	internal	<Any>
11	Deny All	Deny	<Any>	JP/ALL	<Any>	<None>	<Any>	<Any>

The **Interactions** tab displays the access control rules that interact with the current access control rule.

- The current access control rule appears bold.
- Cells that are shaded with a color interact with the current access control rule in a way that might require your attention:
 - **Orange** – Indicates that the cell overlaps with the corresponding cell of the current access control rule
 - **Light green** – Indicates that the cell has a complex relationship with the corresponding cell of the current access control rule (A complex relationship exists when elements contain subsets of each other. For example, if one cell contains [A, B] and another contains [B, C], the cells have a complex relationship because they both include B.)
- Cells that have equal values are not shaded.
- Access control rules that are duplicates of the current access control rule are shaded orange.



Note: For rules that contain no IPv6-compatible applications, the Interactions tab might convert **<Any>** endpoints to **<Any V4>** endpoints.

Create access control rules and groups

Create an access control rule using the access control rule template or base it on an existing access control rule. To organize your access control rules, create access control rule groups.

Select **Policy > Access Control Rules**.



Tip: For option descriptions, click **Help**.

Table 47: Create access control rules and groups tasks

Task	Steps
Create an access control rule using the rule template	<ol style="list-style-type: none"> 1) Click New > New Rule 2) In the Rules: Rule Properties window, configure the access control rule as appropriate, then click OK. 3) Save your changes.
Create an access control rule based on an existing access control rule	<ol style="list-style-type: none"> 1) Select the appropriate access control rule, then click Duplicate. 2) In the Rules: Duplicate Rule window, modify the duplicated access control rule. <ol style="list-style-type: none"> a) In the Name field, type a new name. b) Modify the access control rule options as appropriate. c) Click OK. 3) Save your changes.
Create an access control rule group	<ol style="list-style-type: none"> 1) Click New > New Group. 2) In the Rules: New Group window, configure the access control rule group as appropriate, then click OK. 3) Save your changes.

Related concepts

[Configuring access control rules](#) on page 197

Modify access control rules and groups

Make modifications to a rule such as renaming, enabling or disabling.

Select **Policy > Access Control Rules**.



Tip: For option descriptions, click **Help**.

Table 48: Modify access control rules and groups tasks

Task	Steps
Modify an access control rule or group	<ol style="list-style-type: none"> 1) Select the appropriate access control rule, then click Modify. 2) In the Rules: Rule Properties window, modify the access control rule as appropriate, then click OK. 3) Save your changes.
Rename an access control rule or group	<ol style="list-style-type: none"> 1) Select the appropriate access control rule or group, then click Rename. 2) In the pop-up window, type a new name. 3) Click OK. 4) Save your changes.
Enable an access control rule or group	<ol style="list-style-type: none"> 1) Select the appropriate access control rule or group, then click Enable. 2) Save your changes.
Disable an access control rule or group	<ol style="list-style-type: none"> 1) Select the appropriate access control rule or group, then click Disable. 2) Save your changes.

Arrange access control rules and groups

The order that access control rules appear in is significant.

Perform the tasks in the table to arrange access control rules and groups.

Select **Policy > Access Control Rules**.



Tip: For option descriptions, click **Help**.

Table 49: Arrange access control rules and groups tasks

Task	Steps
Cut and paste an access control rule or group	<ol style="list-style-type: none"> 1) Select the appropriate access control rule or group, then click Cut. 2) Select the item that is directly above where you want to paste the access control rule or group. 3) Click Paste. 4) Save your changes.
Drag and drop an access control rule or group	<ol style="list-style-type: none"> 1) Select the appropriate access control rule or group and drag it to a new position. 2) When the access control rule or group is positioned correctly, drop it. 3) Save your changes.
Use the up and down arrows	<ol style="list-style-type: none"> 1) Select the appropriate access control rule or group, then click Up or Down. 2) Save your changes.

View access control rules and groups



Several options are available to view information about access control rules.

Select **Policy > Access Control Rules**.



Tip: For option descriptions, click **Help**.

Table 50: View access control rules and groups tasks

Task	Steps
View audit data for an access control rule	<ol style="list-style-type: none"> 1) Select the appropriate access control rule, then click the View Audit icon. 2) In the Rules: Audit Viewing window, view audit data for the access control rule. 3) When you are finished, close the Rules: Audit Viewing window.
Search access control rules and groups	<ol style="list-style-type: none"> 1) In the Find field, type your search criteria. 2) Click Find Now. <div style="margin-top: 10px;">  Tip: To reset your search, click Clear. </div>
View the access control rules that are active	<ol style="list-style-type: none"> 1) Click Active Rules. 2) Use the Rules: Active Rules to examine the active access control rules. <div style="margin-top: 10px;">  Tip: To examine an access control rule in detail, select it, then click View. </div>
Export a summary of the access control rules that are active as a comma-separated value (.csv) file	<ol style="list-style-type: none"> 1) Click Active Rules. 2) In the Rules: Active Rules window, click Export (csv). 3) In the Export Rule Data window, specify a save location.
View audit data for an access control rule	<ol style="list-style-type: none"> 1) Select the appropriate access control rule, then click the View Audit icon. The Rules: Audit Viewing window appears and displays audit data for the access control rule. 2) When you are finished, close the Rules: Audit Viewing window.

Modify general settings

Modify the access control rule template and configure which columns are displayed.

Select **Policy > Access Control Rules**.



Tip: For option descriptions, click **Help**.

Table 51: General access control rules settings tasks

Task	Steps
Modify the access control rule template	<ol style="list-style-type: none"> 1) Click New > Update Rule Defaults. 2) In the Rules: Rule Template window, configure the access control rule template as appropriate, then click OK. 3) Save your changes.
Configure which columns are displayed	<ol style="list-style-type: none"> 1) Click Columns. 2) In the Rules: Column Selection window, modify the column settings. <ol style="list-style-type: none"> a) Move the columns you want to hide to the Available columns list. b) Move the columns you want to display to the Show these columns in this order list. c) To change the order of the columns, reorder the Show these columns in this order list. d) Click OK. e) Save your changes.

SSL rules

Contents

- [Configuring SSL rules](#) on page 213
- [Duplicate an SSL rule](#) on page 219
- [Modify SSL rules](#) on page 219
- [Arrange SSL rules](#) on page 220
- [View SSL rules](#) on page 221
- [Configure which columns are displayed](#) on page 222

SSL rules determine whether the firewall decrypts SSL connections.

- SSL connections that match an SSL rule are processed according to that rule.
- SSL connections that do not match an SSL rule are not decrypted.
- Regardless of an SSL rule match, connections must also match an access control rule to pass through the firewall.

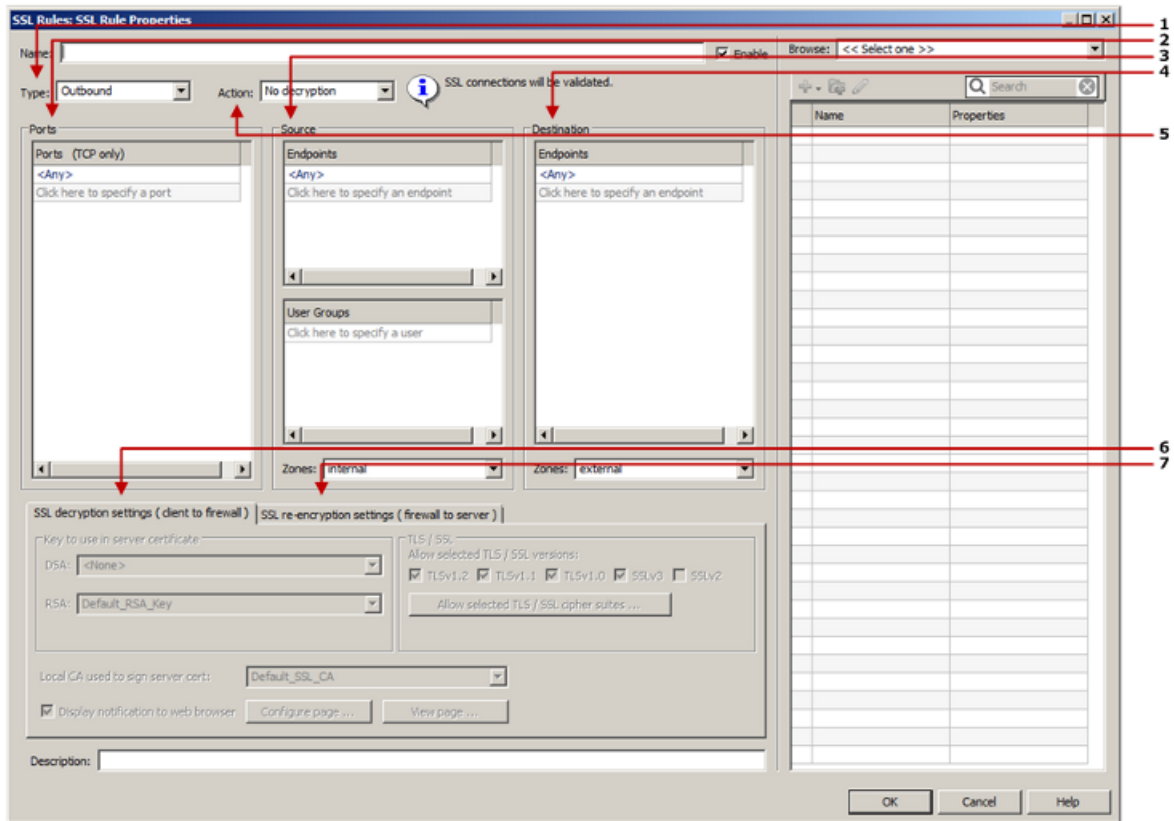
Configuring SSL rules

Consider these main questions when you want to create an SSL rule.

- What connections should the rule match?
- What action should the firewall take on connections that match the rule?

These questions dictate the workflow you must follow to create a new SSL rule. The following table shows this workflow.

Figure 34: Workflow to create an SSL rule



- 1) Type
- 2) Ports
- 3) Source
- 4) Destination
- 5) Action
- 6) SSL decryption settings (client to firewall)
- 7) SSL re-encryption settings (firewall to server)

For example, assume that you want to decrypt, inspect, and re-encrypt outbound HTTPS connections from the HR group. To accomplish this goal, you must create an SSL rule to decrypt and re-encrypt the outbound SSL connections, then create an access control rule to allow and inspect them.

- The following table contains the elements that you must specify on an SSL rule to accomplish this goal.
- To create the basic access control rule that is also required, refer to the related topics.



Note: To select the HR group, this scenario assumes that Passive Passport is configured on the firewall.

Table 52: Required elements

Element	Configuration
Type	Outbound
Action	Decrypt/re-encrypt
Ports	443
Source Endpoints	<Any>
Source Users and Groups	HR
Source Zone	internal
Destination Endpoints	<Any>
Destination Zone	external

In this scenario, you would create an SSL rule based on the elements shown in the table:

- 1) Select **Policy > SSL Rules** and click **New Rule**. The **SSL Rules: SSL Rule Properties** window appears.
- 2) In the **Name** field, type a name for the SSL rule, such as `HR outbound SSL inspection`.
- 3) From the **Type** drop-down list, select **Outbound**.
- 4) From the **Action** drop-down list, select **Decrypt/re-encrypt**.
- 5) In the **Ports** pane, delete **<Any>**, then type `443`.
- 6) In the **Source** area, specify the connection sources to match.
 - a) In the **Endpoints** pane, verify that **<Any>** is specified.
 - b) In the **Users and Groups** pane, select the **HR** group.
 - c) From the **Zone** drop-down list, select **internal**.
- 7) In the **Destination** area, specify the connection destinations to match.
 - a) In the **Endpoints** pane, verify that **<Any>** is specified.
 - b) From the **Zone** drop-down list, select **external**.
- 8) Click the **SSL decryption settings** tab to configure decryption.
 - a) In the **Key to use in server certificate** area, select a public/private key pair to use in the firewall-generated surrogate server certificates that are presented to clients.



Tip: You can select a DSA key pair, an RSA key pair, or both.

- b) From the **Local CA used to sign server cert** drop-down list, select the firewall-hosted CA used to sign the surrogate server certificates that are presented to clients.

- 9) [Optional] Click the **SSL re-encryption settings** tab, then select a CA or group of CAs from the **Trusted CAs** drop-down list.



Tip: The default Trusted Internet CAs group includes most destinations on the Internet.

- 10) Click **OK**, then save your changes.

Related tasks

[Create an SSL rule](#) on page 218

Configuring SSL rule attributes

SSL rules are made up of condition and action elements. Some elements are required for all SSL rules, while the optional elements allow you to tailor rules to meet your specific needs.

Related concepts

[Required elements for SSL rules](#) on page 216

[Optional condition elements for access control rules](#) on page 200

Required elements for SSL rules

The following options must be configured for each SSL rule.

- Name
- Type
- Action
- [Decrypt only and Decrypt/re-encrypt] SSL decryption settings
- [Decrypt/re-encrypt] SSL re-encryption settings

Optional condition elements for SSL rules

The condition elements in the following table are optional. You can configure any of these elements as appropriate to restrict which connections match the SSL rule.

Table 53: Optional condition elements

Optional element	Default configuration	Result of default configuration
Ports	<Any>	SSL connections on any port match.
Source Endpoints	<Any>	All endpoints in the selected source zones match.
Source Users and Groups	None specified	User identity is not used to match connection sources.
Source Zone	<Any>	All selected source endpoints match regardless of which zone contains them.
Destination Endpoints	<Any>	All endpoints in the selected destination zones match.
Destination Zone	<Any>	All selected destination endpoints match regardless of which zone contains them.

Select elements using the browse pane for SSL rules

The browse pane is a multi-function browser that allows you to modify and select elements for the following fields:

- Endpoints
- Zones
- Users and Groups

The browse pane is context-sensitive; different options are displayed based on the field you are browsing.

Select the field you want to browse in either of the following ways:

- Click inside the appropriate field.
- From the **Browse** drop-down list, select the appropriate area.

For example, perform the following steps to select elements for the [Source] Endpoints field.

Steps

- 1) Select the field using one of the following methods:



Tip: For option descriptions, click **Help**.

- Click inside the [Source] Endpoints pane.
- From the **Browse** drop-down list, select **Source endpoints**.

The browse pane switches to the Source endpoints view.

- 2) In the browse pane, you can:

- Select an object by selecting the corresponding checkbox.

- Add, modify, and search objects using the toolbar.

Create an SSL rule

Create and configure an SSL rule.

Steps

- 1) Select **Policy > SSL Rules** and click **New Rule**. The **SSL Rules: SSL Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 2) In the **Name** field, type a name for the SSL rule, such as `HR outbound SSL inspection`.
- 3) Select a type.
 - **Inbound**
 - **Outbound**
 - **<Any>**
- 4) Specify which TCP ports to match.
- 5) Select the sources to match.
 - Select endpoints in the **[Source] Endpoints** pane.
 - Select users and groups in the **[Source] Users and Groups** pane.
 - Select zones and zone groups from the **[Source] Zones** drop-down list.
- 6) Select the destinations to match.
 - Select hosts and SmartFilter URL categories in the **[Destination] Endpoints** pane.
 - Select zones from the **[Destination] Zones** drop-down list.
- 7) Select an action.
 - **No decryption**
 - **Decrypt only**
 - **Decrypt/re-encrypt**
- 8) [Decrypt and Decrypt/re-encrypt] Configure decryption settings.
- 9) [Decrypt/re-encrypt only] Configure re-encryption settings.
- 10) Click **OK**, then save your changes.

Related concepts

[Passive identity validation](#) on page 94

Related tasks

[Duplicate an SSL rule](#) on page 219

[Create an access control rule](#) on page 203

Duplicate an SSL rule

You can copy an existing SSL rule.

Steps

- 1) Select **Policy > SSL Rules**.
- 2) Select the appropriate SSL rule, then click **Duplicate**.



Tip: For option descriptions, click **Help**.

- 3) In the **SSL Rules: SSL Rule Properties** window, modify the duplicated SSL rule.
- 4) In the **Name** field, type a new name.
- 5) Modify the SSL rule options as appropriate.
- 6) Click **OK**.
- 7) Save your changes.

Related tasks

[Create an SSL rule](#) on page 218

Modify SSL rules

Use the tasks in the table to modify SSL rules.



Tip: For option descriptions, click **Help**.

Table 54: Modify SSL rules using these tasks

Task	Steps
Modify an SSL rule	<ol style="list-style-type: none"> 1) Select the appropriate SSL rule, then click Modify. 2) In the SSL Rules: SSL Rule Properties window, modify the SSL rule as appropriate, then click OK. 3) Save your changes.
Rename an SSL rule	<ol style="list-style-type: none"> 1) Select the appropriate SSL rule, then click Rename. 2) In the pop-up window, type a new name. 3) Click OK. 4) Save your changes.
Enable an SSL rule	<ol style="list-style-type: none"> 1) Select the appropriate SSL rule, then click Enable. 2) Save your changes.
Disable an SSL rule	<ol style="list-style-type: none"> 1) Select the appropriate SSL rule, then click Disable. 2) Save your changes.

Arrange SSL rules

Use the tasks in the table to reorder SSL rules.



Tip: For option descriptions, click **Help**.

Table 55: Arrange SSL rules using these tasks

Task	Steps
Cut and paste an SSL rule	<ol style="list-style-type: none"> 1) Select the appropriate SSL rule, then click Cut. 2) Select the item that is directly above where you want to paste the SSL rule. 3) Click Paste. 4) Save your changes.

Task	Steps
Drag and drop an SSL rule	<ol style="list-style-type: none"> 1) Select the appropriate SSL rule and drag it to a new position. 2) When the SSL rule is positioned correctly, drop it. 3) Save your changes.
Use the up and down arrows	<ol style="list-style-type: none"> 1) Select the appropriate SSL rule, then click Up or Down. 2) Save your changes.


View SSL rules

Use the tasks in the table to view SSL rules.



Tip: For option descriptions, click **Help**.

Table 56: View SSL rules using these tasks

Task	Steps
Search SSL rules	<ol style="list-style-type: none"> 1) In the Find field, type your search criteria. 2) Click Find Now. <p> Tip: To reset your search, click Clear.</p>
View audit data for an SSL rule	<ol style="list-style-type: none"> 1) Select the appropriate SSL rule, then click View Audit. The Rules: Audit Viewing window appears and displays audit data for the SSL rule. 2) When you are finished, close the Rules: Audit Viewing window.

Configure which columns are displayed

Configure which columns are displayed on the **SSL Rules** window.

Steps

- 1) Click **Columns**.



Tip: For option descriptions, click **Help**.

- 2) In the **Rules: Column Selection** window, modify the column settings.
 - a) Move the columns you want to hide to the **Available columns** list.
 - b) Move the columns you want to display to the **Show these columns in this order** list.
 - c) To change the order of the columns, reorder the **Show these columns in this order** list.
- 3) Click **OK**.
- 4) Save your changes.

Policy in action

Contents

- [Working with policy](#) on page 223
- [Allowing a custom application](#) on page 224
- [Allowing inbound access to internal servers](#) on page 225
- [Allowing outbound web access](#) on page 233
- [Allowing IPv6 network flows through the firewall](#) on page 236
- [Configure IPv4-to-IPv6 translation for HTTP](#) on page 239
- [Configure non-transparent HTTP](#) on page 243
- [Controlling access based on user identity](#) on page 246
- [Create an alternate policy](#) on page 249
- [Creating SSL content inspection exemptions](#) on page 250
- [Decrypting and inspecting SSH content](#) on page 252
- [Deny access based on country of origin](#) on page 257
- [Deny access to an application category](#) on page 258
- [Discovering which applications are in use in a zone](#) on page 260
- [Examine your policy using the Firewall Policy Report](#) on page 262
- [Inspect and control inbound HTTPS](#) on page 262
- [Inspect and control outbound SSL \(including HTTPS\)](#) on page 266
- [Create a rule to allow traceroute through the firewall](#) on page 271
- [Create a SPAN policy](#) on page 272

Combine elements of policy, such as applications, Application Defenses, network objects, and rules to control traffic through Sidewinder.

Working with policy

The following sections contain policy scenarios that use multiple elements of firewall policy.

For all scenarios, the firewall zones are configured as follows:

- **Protected zone** — internal
- **Internet zone** — external

The following terms are used to describe connections that pass through the firewall:

- *Outbound* connections are those that pass from the protected zone to the Internet zone.
- *Inbound* connections are those that pass from the Internet zone to the protected zone.

Allowing a custom application

Sidewinder allows you to create a custom application to combine the attributes of an existing application with new ports.

Create a custom application if you need to override the ports of an application in the application database.

Scenario:

Assume you want to allow MySQL connections on a non-standard port like TCP 11500. To do so, complete the following tasks.

Related tasks

[Create a custom application based on MySQL](#) on page 224

[Use the custom application in an access control rule](#) on page 225

Create a custom application based on MySQL

Create a custom application based on the MySQL application.

Steps

- 1) Select **Policy > Rule Elements > Applications**.
- 2) Click **New**. The **New Application** window appears.



Tip: For option descriptions, click **Help**.

- 3) Configure the custom application.
 - a) In the **Name** field, type `MySQL on port 11500`.
 - b) In the **Parent application** area, select **other**.
 - c) In the **Search** field, type `MySQL`.
 - d) In the **Select parent application** list, select the **MySQL** application.
 - e) Clear the **TCP ports** field, then type `11500`.
 - f) Click **OK**.
- 4) Save your changes.

Use the custom application in an access control rule

Create an access control rule that uses the custom application you created.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type `Allow MySQL on port 11500`.
- 4) From the **Action** drop-down list, select **Allow**.
- 5) In the **Applications** pane, select **MySQL on port 11500**.
- 6) Configure the **Source** and **Destination** areas as appropriate.
- 7) Click **OK**, then save your changes.

Allowing inbound access to internal servers

To allow inbound access to internal servers, create inbound redirect access control rules. There are two ways to redirect inbound connections.

Related concepts

[Redirecting based on application](#) on page 225

[Redirecting HTTP based on URL](#) on page 228

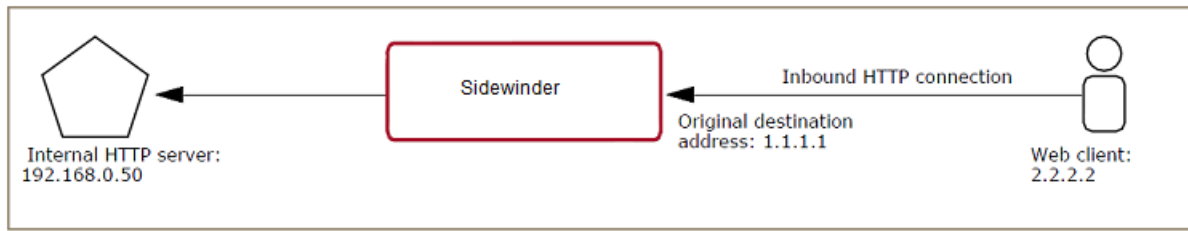
Redirecting based on application

You can configure an inbound redirect rule to forward a connection destined for an external firewall IP address to an internal server. Redirection works based on connection elements such as application, source, and destination.

Scenario:

Assume you want to allow HTTP connections from the Internet to reach an internal HTTP server, as shown by the figure below. The external client (2.2.2.2) initiates a connection to the Sidewinder external IP address (1.1.1.1). The firewall redirects the connection to the appropriate internal server (192.168.0.50).

Figure 35: Redirection in action



The inbound access control rule must redirect the connection to the internal host.

Table 57: Inbound redirect rule

Source zone: external	Destination zone: external
Source endpoint: 2.2.2.2 (external client)	Destination endpoint: 1.1.1.1 (external firewall address)
NAT address: <None>	Redirect: 192.168.0.50 (internal server)

To configure the access control rule shown above, perform these tasks:

Related tasks

[Create network objects](#) on page 226

[Create an inbound redirect access control rule](#) on page 227

Create network objects

Create network objects for the internal HTTP server and the firewall external IP address.

Steps

- 1) Select **Policy > Rule Elements > Network Objects**.
- 2) Create a network object for the internal HTTP server.



Tip: For option descriptions, click **Help**.

- a) Click **New > IP Address**.
 - b) In the **Name** field, type `Internal web server`.
 - c) In the **IP Address** field, type `192.168.0.50`.
- 3) Create a network object for the firewall external IP address.
 - a) Click **New > IP Address**.
 - b) In the **Name** field, type `Firewall external IP`.

- c) In the **IP Address** field, type 1 . 1 . 1 . 1.
- 4) Save your changes.

Create an inbound redirect access control rule

Create an access control rule to redirect inbound HTTP connections to your internal HTTP server.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type a name for the access control rule, such as `Inbound redirect to HTTP server`.
- 4) Make the following selections.

Table 58:

Option	Selection
Action	Allow
Applications	HTTP
[Source] Zone	external
[Destination] Endpoints	Firewall external IP
[Destination] Zone	external
NAT	<None>
Redirect	Internal web server

- 5) Click **OK**.
- 6) Position the new access control rule above the **Deny All** rule.
- 7) Save your changes.

Redirecting HTTP based on URL

Use URL translation to configure your firewall to redirect inbound HTTP connections based on the URL contained in the HTTP request.

By examining the HTTP application layer data, the firewall determines which internal web server inbound requests are destined for even if multiple servers share the same external IP address, as is common in virtual hosting environments.

Use URL translation if your network environment matches one or more of the following scenarios:

- You have multiple web sites that resolve via DNS to a single IP on your firewall.
- You have a website that contains resources that are hosted on different physical servers behind your firewall.

URL translation is not compatible with:

- Inbound SSL content inspection
- IPv6 connections



Note: If an IPv6 connection matches a URL translation rule, the connection is dropped and an error is audited.

If URL translation is enabled on an internet-facing zone, inbound HTTP requests are handled as follows:

- 1) An inbound HTTP request reaches the firewall.



Note: The TCP connection must be destined for an IP address that is assigned to the firewall.

- 2) The firewall examines the HTTP request's application layer data and compares it to the defined URL translation rules to determine which internal web server the request should be sent to.
- 3) [If **Rewrite URL** is enabled] The firewall rewrites the application data in the HTTP request as configured so that it conforms to the requirements of the internal web server.
- 4) Based on the IP address of the destination web server determined in step 2, an access control rule match is performed.
 - If an access control rule matches, the connection is redirected to the internal web server.
 - If no access control rules match, the connection is denied.

Manage URL translation rules

Create URL translation rules to redirect inbound HTTP connections based on application layer data.

Steps

- 1) Select **Policy > Application Defenses > Defenses > HTTP**.

- 2) Click **URL Translation Rules**. The **URL Translation Rules** window appears.



Tip: For option descriptions, click **Help**.

The **URL Translation Rules** table lists the configured URL translation rules. The URL translation rules are checked in order and the first rule that matches is used. For this reason, more specific rules should be placed higher in the rules list. Use the up and down arrows to change the rule order. To manage the URL translation rules, use the following buttons:

- **New** — Create a new URL translation rule.
- **Modify** — Edit an existing URL translation rule. You can also double-click a rule to modify it.
- **Delete** — Delete the selected URL translation rule.
- **Duplicate** — Copy the selected URL translation rule.
- **Rename** — Rename the selected URL translation rule.

When you create URL translation rules, consider these guidelines:

- Order your rules so that the most specific rules are placed first.
- Avoid using file names in the **Path Prefix** fields.
- Avoid adding trailing slashes to paths you specify in the **Path Prefix** fields. Path prefix matches are exact, so a trailing slash can cause unwanted behavior. For example, specifying `/directory_name/` in the **Path Prefix** does not match the request `GET /directory_name` because the trailing slash is missing.



Note: Performing URL translation and conventional redirection for the same firewall IP address is not supported.

Create a URL translation rule

Configure inbound HTTP access to an internal web server using URL Translation.

Steps

- 1) Click **New**.



Tip: For option descriptions, click **Help**.

The **New URL Translation Rule** window appears.

- 2) In the **Name** field, type a descriptive name for this rule.
- 3) [Optional] In the **Description** field, enter any useful information about this rule.
- 4) In the **Client Source** area, choose the zone or zones where the clients that generate the inbound HTTP requests are located by doing one of the following:
 - Select **Zones**, then select the appropriate zone or zones from the list.
 - Select **Zonegroups**, then select the appropriate zone group or groups from the list.
- 5) In the **Original URL** area, configure the HTTP matching parameters by doing one of the following:
 - Select **Matching URL** and type the URL that this rule should match. To specify a custom port, add the port to the end of the URL. Example: `http://example.net:3128`.

The **Host**, **Ports**, and **Path Prefix** fields are automatically populated based on the URL you enter.

- Select **Matching URL attributes** and complete the **Host**, **Ports**, and **Path Prefix** fields with the data used to match inbound HTTP requests.
- 6) In the **New Server Destination** area, select or create an IP address object that corresponds to the internal web server that connections matching this rule should be redirected to.
 - 7) [Optional] Select **Rewrite URL** if you need to translate the inbound HTTP request so that it matches the host name and path structure of the internal web server.



Note: The new URL information replaces only the original URL information you entered in Step 6. Path information beyond the original URL path prefix in the HTTP request is unaffected.

Select an option:

- Select **New URL**, then type the URL that should replace the original URL. To specify a different port, deselect the **Maintain original port** checkbox and add the port to the end of the URL. Example: `http://example.net:3128`.
The **Host**, **Ports**, and **Path Prefix** fields below are automatically populated based on the URL you enter.
- Select **New URL attributes**, then complete the **Host**, **Ports**, and **Path Prefix** fields with the data to replace the original URL attributes.



Note: Sidewinder does not modify hyperlinks in HTML files, so web servers that the firewall performs URL translation for should employ relative links whenever possible. The firewall does translate the Location header in 3xx redirection server status codes.

- 8) Click **Add**. You return to the **HTTP Proxy Agent Properties** window.
- 9) Click **OK** and save your changes.

Create an access control policy to authorize inbound HTTP

URL translation rules only determine the internal IP address to redirect the inbound HTTP requests to. Access control rules are required to authorize inbound connections based on the information in the URL translation rules.

To create the required access control policy, perform these tasks.

Create a Generic Application Defense profile for inbound URL translation

Create a Generic Application Defense profile to enable the non-transparent connection type for HTTP.

Steps

- 1) Select **Policy > Application Defenses > Defenses > Generic (Required)**.

- 2) Click **New**. A pop-up window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the new profile, such as `Inbound URL Translation`, then click **OK**.
- 4) Confirm that the new profile is selected, then click **Connection Settings**.
- 5) In the new window, enable the non-transparent connection type for HTTP.
 - a) Select **Override default connection types**.
 - b) From the **HTTP** drop-down list, select **non-transparent**.
 - c) Click **OK**.
- 6) Save your changes.

Create an HTTP Application Defense profile for inbound URL translation

Create an HTTP Application Defense profile to configure enforcement settings for HTTP.

Steps

- 1) Select **Policy > Application Defenses > Defenses > HTTP**.

- 2) Click **New**. A pop-up window appears.



Tip: For option descriptions, click **Help**.

- 3) Define the new profile.
 - a) Type a name for the new profile, such as `Inbound URL Translation`.
 - b) From the **Select a Type of Web Application Defense** drop-down list, select **Server**.
 - c) Click **OK**.
- 4) [Optional] Configure enforcement settings.
 - a) In the **Enforcements** tab, enable HTTP enforcements as appropriate.
 - b) Use the other tabs to configure the enabled enforcements.
- 5) Save your changes.

Create an Application Defense group for inbound URL translation

Create an Application Defense group that contains the Generic and HTTP Application Defense profiles you created. The group will be used by an access control rule.

Steps

1) Select **Policy > Application Defenses > Groups**.

2) Click **New**. A pop-up window appears.



Tip: For option descriptions, click **Help**.

3) Type a name for the new Application Defense group, such as `Inbound URL Translation group`, then click **OK**.

4) Select the profiles that you created.

a) Confirm that the new Application Defense group is selected in the upper pane.

b) From the **Generic (Required)** drop-down list, select the Generic Application Defense profile you created.

c) From the **HTTP** drop-down list, select the HTTP profile you created.

5) Save your changes.

Create an access control rule for inbound URL translation

Create an access control rule that uses the Application Defense group you created.

Steps

1) Select **Policy > Access Control Rules**.

2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

3) In the **Name** field, type `Inbound URL Translation`.

4) Make the following selections

Option	Selection
Action	Allow
Applications	HTTP
[Source] Zone	external
[Destination] Endpoints	Select all internal HTTP servers that URL translation rules redirect connections to
[Destination] Zone	internal (the zone where the destination servers are located)
Redirect	<None>
Application Defense	Inbound URL Translation group

- 5) [Optional] If you added ports other than 80 to any URL translation rules, add them to the list of ports.
 - a) From the ports drop-down list, select **Override ports**.
 - b) In the text box, type the additional ports.
- 6) Click **OK**.
- 7) Position the new access control rule so that it is above the **Deny All** rule.
- 8) Save your changes.

Allowing outbound web access

Sidewinder can inspect and control HTTP and HTTPS, which are the protocols most commonly used to access the web.

However, because HTTPS uses SSL encryption, the firewall cannot distinguish HTTPS from other SSL-encapsulated applications without performing decryption. Therefore, you have two options to allow outbound HTTPS:

- **SSL pass-through** — Create access control rules that use the SSL/TLS application to allow outbound SSL. The SSL/TLS application matches all SSL connections on port 443, including HTTPS and other SSL-encapsulated applications.
- **SSL content inspection** — Configure SSL rules to decrypt SSL connections, then use access control rules to control the decrypted SSL.

Related tasks

[Allow HTTP and pass-through SSL \(including HTTPS\) on page 234](#)

[Allow HTTP only on page 234](#)

[Allow pass-through SSL only on page 235](#)

[Inspect and control outbound SSL \(including HTTPS\) on page 266](#)

Allow HTTP and pass-through SSL (including HTTPS)

Assume that you want to allow outbound HTTP and pass-through SSL (including HTTPS). To do so, create an access control rule that uses the HTTP and SSL/TLS applications.

To allow outbound HTTP and SSL/TLS, you can also enable the default Internet Services access control rule. To create an access control rule that uses the HTTP and SSL/TLS applications:

Steps

1) Select **Policy > Access Control Rules**.

2) Click **New > New Rule**.

The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

3) In the **Name** field, type **Outbound HTTP and SSL**.

4) Make the following selections.

Option	Selection
Action	Allow
Applications	<ul style="list-style-type: none"> • HTTP • SSL/TLS
[Source] Zone	internal
[Destination] Zone	external

5) Click **OK**.

6) Position the new access control rule above the **Deny All** rule.

7) Save your changes.

Allow HTTP only

Create an access control rule to allow HTTP and override the default ports.

Assume that you want to allow HTTP but not HTTPS or SSL. Overriding the ports to remove SSL/443 prevents the rule from matching HTTPS connections that are decrypted by an SSL rule.

Steps

1) Select **Policy > Access Control Rules**.

- 2) Click **New > New Rule**.
The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type `Outbound HTTP` only.
- 4) Make the following selections.

Option	Selection
Action	Allow
Applications	HTTP
[Source] Zone	internal
[Destination] Zone	external

- 5) To prevent the rule from matching decrypted HTTPS connections on port 443, override the application ports.
 - a) From the ports drop-down list, select **Override ports**.
 - b) Clear the text box, then type `TCP/80`.
- 6) Click **OK**.
- 7) Position the new access control rule above the **Deny All** rule.
- 8) Save your changes.

Allow pass-through SSL only

Assume that you want to allow SSL to pass through the firewall without inspecting it. To do so, create an access control rule that uses the SSL/TLS application.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**.
The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type `Outbound SSL` only.

- 4) Make the following selections.

Option	Selection
Action	Allow
Applications	SSL/TLS
[Source] Zone	internal
[Destination] Zone	external

- 5) Click OK.
- 6) Position the new access control rule above the **Deny All** rule.
- 7) Save your changes.

Allowing IPv6 network flows through the firewall

This section describes how to create a rule that allows IPv6 network flow through the firewall. Use these scenarios as examples when creating IPv6 allow rules for other applications.

- **Allow HTTP over IPv6** — For an application with native IPv6 support (HTTP)
- **Allow SSH over IPv6** — For an application that lacks native IPv6 support (SSH).

Related tasks

[Allow HTTP over IPv6 on page 236](#)

[Allow SSH over IPv6 on page 237](#)

Allow HTTP over IPv6

Use this task to allow only outbound HTTP IPv6 network flows through the firewall. You can use the same approach for other applications that natively support IPv6.



Note: By default, IPv6 is enabled.

Steps

- 1) Select **Policy > Access Control Rules..**
The **Access Control Rules** page appears.
- 2) Click **New > New Rule.**
The **Rules: Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type **Allow HTTP over IPv6**.
- 4) In the **Rules: Rule Properties** window, configure the access control rule.



Note: Key selections are highlighted in bold.

Table 59: Allow HTTP over IPv6 access control rule

Option	Selection
Action	Allow
Application	HTTP
[Source] Endpoint	<Any V6>
[Source] Zone	internal
[Destination] Endpoint	<Any V6>
[Destination] Zone	external

- 5) Click **OK**.
- 6) Position the new access control rule above the **Deny All** rule.
- 7) Save your changes.

Related reference

[Firewall IPv4 and IPv6 support by area](#) on page 364

Allow SSH over IPv6

Use this task to allow only outbound SSH IPv6 network flows through the firewall. You can use the same approach for other applications that lack native IPv6 support.

This task has two parts.

Create a custom TCP application

Use this task to create a custom application based on TCP that uses the standard SSH port.

Steps

- 1) Select **Policy > Rule Elements > Applications**.

- 2) Click **New**. The **New Application** window appears.



Tip: For option descriptions, click **Help**.

- 3) Configure the custom application.
 - a) In the **Name** field, type `TCP on port 22`.
 - b) In the Parent application area, select **TCP/UDP**.
 - c) In the **TCP ports** field, type `22`.
 - d) Click **OK**.
- 4) Save your changes.

Create an allow rule for the custom TCP application

Create an IPv6 allow rule that uses the custom application.



Note: By default, IPv6 is enabled.

Steps

- 1) Select **Policy > Access Control Rules**. The **Access Control Rules** page appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New > New Rule**. The **Rules: Rule Properties** window appears.
- 3) In the **Name** field, type `Allow SSH over IPv6`.

- In the **Rules: Rule Properties** window, configure the access control rule.



Note: Key selections are highlighted in **bold**.

Table 60: Allow SSH over IPv6 access control rule

Option	Selection
Action	Allow
Application	TCP on Port 22(custom application)
[Source] Endpoint	<Any V6>
[Source] Zone	internal
[Destination] Endpoint	<Any V6>
[Destination] Zone	external

- Click **OK**.
- Position the new access control rule above the **Deny All** rule.
- Save your changes.

Related reference

[Firewall IPv4 and IPv6 support by area](#) on page 364

Configure IPv4-to-IPv6 translation for HTTP

An IPv4 client cannot directly connect to an IPv6 server through the firewall. However, you can configure an access control rule to allow an IPv4 client to connect to HTTP-based applications on an IPv6 server.

The following conditions must be met:

- The connection from the IPv4 client to the firewall must be non-transparent HTTP (NT-HTTP).



Tip: The client browsers must be configured to use the firewall IP address as a proxy server.

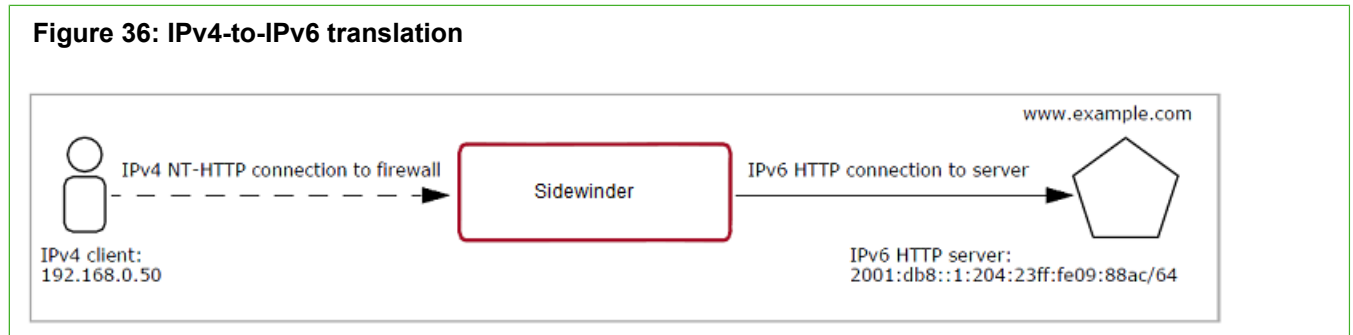
- The firewall must be assigned an IPv6 address in the zone where the IPv6 HTTP server is located.
- The firewall must be able to resolve the host name of the HTTP server to IPv6 address using DNS. If any IPv4 addresses exist for the server, translation is not performed and the connection between the firewall and the server is made using IPv4.

Scenario:

Assume that you want to allow an IPv4 client to reach an IPv6 web server at www.example.com.

In the figure below, an IPv4 client sends a non-transparent HTTP request for www.example.com to the firewall. Because www.example.com resolves to an IPv6 address, the firewall makes an IPv6 HTTP connection to the

server to retrieve www.example.com on behalf of the client. The table below shows the required IPv4-to-IPv6 translation rule.



The translation rule must:

- Use the HTTP application
- Allow non-transparent HTTP connections
- Allow IPv6 destination endpoints
- NAT the connection to a firewall IPv6 address

Table 61: Example IPv4-to-IPv6 access control rule

Applications: HTTP	Action: Allow
Source zone: internal	Destination zone: external
Source endpoint: 192.168.0.50 (internal client)	Destination endpoint: 2001:db8::1:204:23ff:fe09:88ac/64 (external HTTP server)
NAT address: <localhost> (firewall external IPv6 address)	Redirect: <None>

To configure HTTP IPv4-to-IPv6 translation, perform the following tasks.

Create a Generic Application Defense profile for IPv4 to IPv6 translation

Create a Generic Application Defense profile to enable the non-transparent connection type for HTTP.

Steps

- 1) Select **Policy > Application Defenses > Defenses > Generic (Required)**.
- 2) Click **New**. A pop-up window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the new profile, such as **HTTP IPv4-to-IPv6**, then click **OK**.
- 4) Confirm that the new profile is selected, then click **Connection Settings**.

- 5) In the new window, enable the non-transparent connection type for HTTP.
 - a) Select **Override default connection types**.
 - b) From the **HTTP** drop-down list, select **non-transparent**.



Tip: If you select **both**, transparent HTTP connections might match access control rules that use this profile. However, IPv4-to-IPv6 translation is not performed for transparent connections.

- c) Click **OK**.
- 6) Save your changes.

Create an HTTP Application Defense profile for IPv4 to IPv6 translation

Create an HTTP Application Defense profile to configure enforcement settings for HTTP.

Steps

- 1) Select **Policy > Application Defenses > Defenses > HTTP**.
- 2) Click **New**. A pop-up window appears.



Tip: For option descriptions, click **Help**.

- 3) Define the new profile.
 - a) Type a name for the new profile, such as `Outbound HTTP`.
 - b) From the **Select a Type of Web Application Defense** drop-down list, select **Client**.
 - c) Click **OK**.
- 4) [Optional] Configure enforcement settings.
 - a) On the **Enforcements** tab, enable HTTP client enforcements as appropriate.
 - b) Use the other tabs to configure the enabled enforcements.
- 5) Save your changes.

Create an Application Defense group for IPv4 to IPv6 translation

Create an Application Defense group that contains the Generic and HTTP profiles that you created. The group will be used by an access control rule.

Steps

- 1) Select **Policy > Application Defenses > Groups**.
- 2) Click **New**. A pop-up window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the new Application Defense group, such as `HTTP IPv4-to-IPv6 group`, then click **OK**.
- 4) Select Application Defense profiles.
 - a) Confirm that the new Application Defense group is selected in the upper pane.
 - b) From the **Generic (Required)** drop-down list, select the Generic profile that you created.
 - c) From the **HTTP** drop-down list, select the HTTP profile that you created.
- 5) Save your changes.

Create an access control rule for IPv4 to IPv6 translation

Create an access control rule that uses the Application Defense group you created.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type `Outbound HTTP IPv4-to-IPv6`.
- 4) From the **Action** drop-down list, select **Allow**.
- 5) In the **Applications** pane, select **HTTP**.
- 6) [Optional] To allow non-transparent HTTPS connections on port 80, add **SSL/80** to the list of ports.
 - a) From the ports drop-down list, select **Override ports**.

b) In the text box, type `TCP/80 SSL/80,443`.

7) Configure the **Source** and **Destination** areas as appropriate.

- The source endpoints must match IPv4 clients.
- The destination endpoints must match IPv6 destinations.



Tip: To match all IPv6 destinations, select `<Any V6>`.

8) Configure **Advanced** options.

- a) From the **Application Defense** drop-down list, select the Application Defense group you created.
- b) From the **NAT** drop-down list, select the firewall external IPv6 address.



Tip: If the primary external firewall address is IPv6, you can select `<localhost>`.

9) Click **OK**, then save your changes.

Configure non-transparent HTTP

Sidewinder can be configured to accept non-transparent HTTP connections. In this configuration, the firewall functions as a proxy server.

Scenario:

Assume that you want to configure the firewall to function as a proxy server for internal clients.

To configure non-transparent HTTP, perform the following tasks.



Note: SSL content inspection cannot be performed for non-transparent HTTP connections.

Create a Generic Application Defense profile for non-transparent HTTP

Create a Generic Application Defense profile to enable the non-transparent connection type for HTTP.

Steps

- 1) Select **Policy > Application Defenses > Defenses > Generic (Required)**.
- 2) Click **New**. A pop-up window appears.
- 3) Type a name for the new profile, such as `Non-transparent HTTP`, then click **OK**.
- 4) Confirm that the new profile is selected, then click **Connection Settings**.

- 5) In the new window, enable the non-transparent connection type for HTTP.
 - a) Select **Override default connection types**.
 - b) From the **HTTP** drop-down list, select **non-transparent**.



Tip: When you select **non-transparent**, transparent (normal) HTTP connections will not match access control rules that use this profile.

- c) Click **OK**.
- 6) Save your changes.

Create an HTTP Application Defense profile for non-transparent HTTP

Create an HTTP Application Defense profile to configure enforcement settings for HTTP.

Steps

- 1) Select **Policy > Application Defenses > Defenses > HTTP**.
- 2) Click **New**. A pop-up window appears.



Tip: For option descriptions, click **Help**.

- 3) Define the new profile.
 - a) Type a name for the new profile, such as `Outbound HTTP`.
 - b) From the **Select a Type of Web Application Defense** drop-down list, select **Client**.
 - c) Click **OK**.
- 4) [Optional] Configure enforcement settings.
 - a) On the **Enforcements** tab, enable HTTP client enforcements as appropriate.
 - b) Use the other tabs to configure the enabled enforcements.
- 5) Save your changes.

Create an Application Defense group for non-transparent HTTP

Create an Application Defense group that contains the Generic and HTTP Application Defense profiles you created. The group will be used by an access control rule.

Steps

- 1) Select **Policy > Application Defenses > Groups**.
- 2) Click **New**. A pop-up window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the new Application Defense group, such as `Non-transparent HTTP group`, then click **OK**.
- 4) Select the profiles that you created.
 - a) Confirm that the new Application Defense group is selected in the upper pane.
 - b) From the **Generic (Required)** drop-down list, select the Generic Application Defense profile you created.
 - c) From the **HTTP** drop-down list, select the HTTP profile you created.
- 5) Save your changes.

Create an access control rule for non-transparent HTTP

Create an access control rule that uses the Application Defense group you created.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type a name for the access control rule, such as `Outbound non-transparent HTTP`.
- 4) From the **Action** drop-down list, select **Allow**.
- 5) Select the applications to match.
 - a) In the **Applications** pane, select **HTTP**.

- b) [Optional] To allow non-transparent HTTPS connections, select **SSL/TLS**.
- 6) [Optional] To allow non-transparent HTTPS connections on port 80, add SSL/80 to the list of ports.
 - a) From the ports drop-down list, select **Override ports**.
 - b) In the text box, type `TCP/80 SSL/80,443`.



Tip: If the client browsers are configured to use a custom port for the proxy, add the port to the list of ports. Example: For port 9119, type `TCP/80,9119 SSL/80,443,9119`.

- 7) Configure the **Source** and **Destination** areas as appropriate.
- 8) In the **Advanced** pane, select the Application Defense group you created from the **Application Defense** drop-down list.
- 9) Click **OK**, then save your changes.

Controlling access based on user identity

Sidewinder allows you to create access control rules and SSL rules that match the users and groups in your Windows domain.



Note: To create user-based policy, passive identity validation must be configured on your firewall.

Related concepts

[Passive identity validation](#) on page 94

[Benefits of SmartFilter](#) on page 136

Related tasks

[Enforce SmartFilter URL filtering for the Sales group](#) on page 246

[Exempt the Sales manager from URL filtering](#) on page 249

Enforce SmartFilter URL filtering for the Sales group

Assume that you want to enforce URL filtering for the Sales group. Perform these tasks.

Configure a SmartFilter filter policy

To control which websites are allowed, denied, and exempt, configure a filter policy.

Steps

1) Select **Policy > Application Defenses > SmartFilter**.

2) Click the **Filter Policies** tab.



Tip: For option descriptions, click **Help**.

3) Examine the default filter policies.

- If one of default filter policies meets your needs, continue to the next procedure. For example, the *Typical_Business_Filter* blocks categories that are generally not business-related.
- To create a custom filter policy, click **New**.

Select the filter policy in an HTTP Application Defense profile

Create an HTTP Application Defense profile that uses the appropriate filter policy.

Steps

1) Select **Policy > Application Defenses > Defenses > HTTP**.

2) Click **New**. A pop-up window appears.



Tip: For option descriptions, click **Help**.

3) Define the new profile.

- a) Type a name for the new profile, such as `Sales URL Filtering`.
- b) From the **Select a Type of Web Application Defense** drop-down list, select **Client**.
- c) Click **OK**.

4) On the **Enforcements** tab, select **SmartFilter**.

5) Select a SmartFilter filter policy.

- a) Click the **SmartFilter** tab.
- b) From the **Filter Policy** drop-down list, select the appropriate filter policy, such as *Typical_Business_Filter*.

6) Save your changes.

Create an Application Defense group for URL filtering

Create an Application Defense group that contains the HTTP profile you created.

Steps

1) Select **Policy > Application Defenses > Groups**.

2) Click **New**. A pop-up window appears.



Tip: For option descriptions, click **Help**.

3) Type a name for the new Application Defense group, such as `Sales URL filtering group`, then click **OK**.

4) Select the HTTP profile you created.

a) Confirm that the new Application Defense group is selected in the upper pane.

b) From the **HTTP** drop-down list, select **Sales URL Filtering**.

5) Save your changes.

Create an access control rule for URL filtering

Create an access control rule that uses the Application Defense group you created.

Steps

1) Select **Policy > Access Control Rules**.

2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

3) In the **Name** field, type `Sales URL Filtering`.

4) From the **Action** drop-down list, select **Allow**.

5) In the **Applications** pane, select **HTTP**.

6) In the **[Source] Users and Groups** pane, select **Sales**.

7) Select the Application Defense group you created.

a) If necessary, expand the **Advanced** pane.

b) From the **Application Defense** drop-down list, select **Sales URL Filtering group**.

- 8) Click **OK**, then save your changes.

Exempt the Sales manager from URL filtering

Create an access control rule to exempt users from URL filtering.

Assume that you want to exempt John Smith, the Sales department manager, from URL filtering. To do so, create an access control rule that:

- Matches his identity
- Does not use SmartFilter

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type `Exempt Sales Manager`.
- 4) From the **Action** drop-down list, select **Allow**.
- 5) In the **Applications** pane, select **HTTP**.
- 6) In the **[Source] Users and Groups** pane, select John Smith's identity.
 - a) From the **Browse** drop-down list, select **Source users and groups**.
 - b) Click the **Users** tab.
 - c) Click **MLC**. The list of users appears.
 - d) In the list of users, select **John Smith**.
- 7) Click **OK**.
- 8) Arrange the new rule so that it is above the **Sales URL Filtering** rule, then save your changes.

Create an alternate policy

Preparing policies for different disaster recovery scenarios can save valuable time in a crisis. Many organizations need an alternate policy that can be implemented quickly, such as a policy that limits inbound access if an attack is discovered.

Assume that you want to create an alternate policy to use in the event of an attack. To do so:

Steps

- 1) Create an access control rule group for the alternate policy.



Tip: For option descriptions, click **Help**.

- 2) In that group, place all the access control rules needed to implement that policy.



Tip: Groups can nest within groups.

- 3) Create a Deny All rule as the last rule of the alternate policy.
- 4) Once the alternate policy is finished, disable it by selecting the main group and clicking **Disable**.
- 5) When you need to use the policy, move the group to the top of the access control rules and enable it. The firewall begins enforcing your alternate policy.

Creating SSL content inspection exemptions

You can create SSL rules to exempt connections from matching subsequent SSL rules.

You might create exemptions for:

- Sensitive applications, such as online banking
- Applications that do not support decryption
 - Applications that do not currently support SSL decryption are listed in Knowledge Base article [9298](#).
- Use elements like TCP ports and endpoints to single out unsupported applications.

Related tasks


[Exempt the finance and banking URL category](#) on page 250

[Exempt an application based on port](#) on page 251

Exempt the finance and banking URL category

Create an SSL rule to prevent connections to confidential sites.

Assume that you want to prevent connections to finance and banking sites from being decrypted. To do so, create the following SSL rule:

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Policy > SSL Rules**.

- 2) Click **New Rule**. The **SSL Rule Properties** window appears.
- 3) In the **Name** field, type `Exempt finance and banking`.
- 4) Make the following selections.


Option	Selection
Type	Outbound
Action	No Decryption
Ports	<Any>
[Destination] Endpoints	Finance/Banking (URL category)

- 5) Click **OK**.
- 6) Position the new SSL rule so that it is above the decryption rules you are exempting connections from matching.
- 7) Save your changes.

Exempt an application based on port

Create an SSL rule to exempt port 7070 for this scenario.

Assume that you want to exempt an application that uses TCP port 7070 from being decrypted.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Policy > SSL Rules**.
- 2) Click **New Rule**. The **SSL Rule Properties** window appears.
- 3) In the **Name** field, type `Exempt port 7070`.
- 4) Make the following selections.

Option	Selection
Type	<Any>
Action	No Decryption
Ports	7070

- 5) Click **OK**.
- 6) Position the new SSL rule so that it is above the decryption rules you are exempting connections from matching.

- 7) Save your changes.

Decrypting and inspecting SSH content

Sidewinder can decrypt SSH connections, perform content inspection, then re-encrypt the traffic before sending it to its destination.

To decrypt and re-encrypt SSH traffic, the firewall:

- Acts like a server when communicating with the client
- Acts like a client when communicating with the server

The firewall maintains two databases to store SSH host keys:

- A known hosts database to store SSH server keys
- A database of SSH server keys to present to clients

Understanding the SSH known host keys trust relationship

The SSH protocol relies on users to decide if the server host keys presented to them are valid. Because the firewall acts like a client when it communicates with SSH servers, server host keys are stored in the firewall's SSH known host keys database.

To distinguish between server host keys that have been administrator-approved and those that have not, the firewall classifies each host key by trust level. The trust level configured for each SSH known host key represents your level of confidence that the host key belongs to the host (IP address) that it claims to belong to. There are two trust levels:

- **Strong** — SSH host keys are considered strong if they have been imported into the SSH known hosts database by administrators or promoted to strong trust level by administrators.
- **Weak** — SSH host keys are considered weak if they are accepted by users without administrator intervention during the initiation of an SSH session.

When you configure the SSH content inspection, you can decide what SSH host key trust level to require in order to allow the SSH connection to take place. For example:

- Enforce **Strict** key checking policy for rules that allow access to critical network security devices. Host keys with strong trust level must already exist in the known hosts database for the security devices that the rule allows access to. These host keys must also pass cryptographic checks for authenticity.
- Enforce **Medium** key checking policy for rules that allow access to non-critical hosts. Host keys with strong or weak trust level are allowed. If a host key is not present in the known hosts database, the client can accept it, which adds the host key to the known hosts database.
- Allow **Relaxed** key checking policy for rules not related to business operations, such as a rule allowing access to an employee's personal computer at home. Host keys with strong or weak trust level are allowed. If a host key is not present in the known hosts database, the client can accept it, which adds the host key to the known hosts database. If a server's host key has changed, the client can accept it, which replaces the old key in the known hosts database.

By tailoring key checking policy to the security risk involved, you can ensure that SSH host keys from critical servers receive administrator verification, while less critical SSH servers can be accessed without administrator intervention.

Strong host key scenario

Presume an SSH client needs to connect to a network security device through the firewall. The network security device is critical for the integrity of the network, so the administrator chooses to enforce strict key checking policy. As a result, the administrator needs to make sure that there is a strong known host key for the network security device in the firewall's known hosts database.

The following configuration steps are necessary to allow the connection to take place:

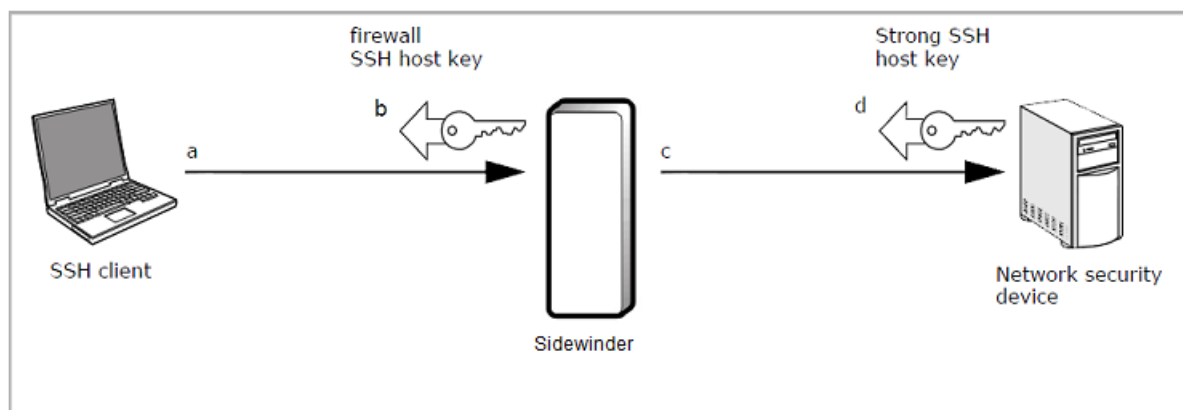
- 1) Configure Application Defenses to specify strict key checking policy.



Note: Create an SSH Application Defense profile that enforces **Strict** key checking policy. This requires a strong host key to be present in the SSH known host keys database for the destination SSH server.

- 2) Create an Application Defense group that contains the SSH profile you created.
- 3) Create an access control rule to allow the SSH client to connect to the network security device. The rule must use the following:
 - SSH application
 - Application Defense group you created
- 4) Import the network security device's SSH host key into the firewall SSH known host keys database and assign the key strong trust level.

Figure 37: Example strong SSH known host key scenario



The figure shows what happens when the SSH client initiates an SSH session to the network security device through the firewall's SSH proxy agent.

- The client initiates an SSH connection to the network security device. The firewall, acting like an SSH server, accepts the client's connection.
- The firewall sends its SSH host key to the client.

- The firewall, acting like an SSH client, initiates an SSH connection to the network security device. The network security device accepts the firewall's connection.
- The network security device sends the firewall its SSH host key.

The firewall examines the SSH host key from the network security device and allows the connection. Because the administrator imported a strong SSH host key for the network security device into the firewall's SSH known hosts database, the requirements of strict key checking policy are met.

Related tasks

[Manage known host keys](#) on page 255

Weak host key scenario

Presume that an employee wants to connect to their home computer through the firewall. The employee's home computer is not critical for the integrity of the network, so the administrator chooses to enforce relaxed key checking policy. As a result, the administrator does not need to import or approve the SSH host key that belongs to the employee's home computer.

The following configuration steps are necessary to allow the connection:

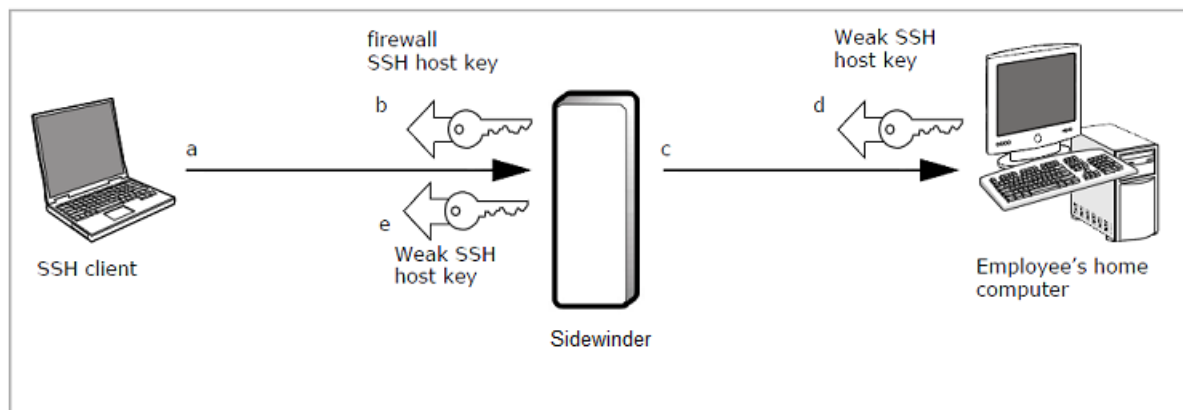
- 1) Configure Application Defenses to specify relaxed key checking policy.



Note: Create an SSH Application Defense profile that enforces **Relaxed** key checking policy. This allows host keys with a strong or weak trust level. If a host key is not present in the known hosts database, the client can accept it, which adds the host key to the known hosts database. If a server host key has changed, the client can accept it, which replaces the old key in the known hosts database.

- 2) Create an Application Defense group that contains the SSH profile you created.
- 3) Create an access control rule to allow the SSH client to connect to the employee's home computer. The rule must use the following:
 - SSH application
 - Application Defense group you created

Figure 38: Example weak SSH known host key scenario



The figure shows what happens when the SSH client initiates an SSH session to the employee's home computer through the firewall's SSH proxy agent.

- 1) The client initiates an SSH connection to the employee's home computer. The firewall, acting like an SSH server, accepts the client connection.
- 2) The firewall sends its SSH host key to the client.
- 3) The firewall, acting like an SSH client, initiates an SSH connection to the employee's home computer. The employee's home computer accepts the firewall connection.
- 4) The employee's home computer sends the firewall its SSH host key.
- 5) The firewall sends the SSH host key presented by the employee's home computer to the client for approval.

The firewall allows the connection if the user approves the SSH host key presented by the employee's home computer. Since the administrator configured relaxed key checking policy for the SSH Application Defense, the user has the ability to approve any SSH host key.

Manage SSH known hosts

Use these steps to manage SSH known host keys.

Steps

- 1) Select **Policy > Application Defenses > Defenses > SSH**.
- 2) Click **SSH Known Hosts**. The **SSH Proxy Agent Properties** window appears.



Tip: For option descriptions, click **Help**.

The **SSH Proxy Agent Properties** window has two tabs:

- **SSH Known Hosts** — Use this tab to manage the database of known host keys.



Note: To configure this tab, an access control rule for the SSH application must be enabled and positioned above the **Deny All** rule.

- **SSH Server Keys** — Use this tab to manage SSH keys that the proxy presents to SSH clients.

Related concepts

[Managing keys](#) on page 634

Manage known host keys

Perform these tasks to manage known host keys.

- Add a known host key by clicking **New** and entering the appropriate information in the pop-up window.
- Modify a known host key by selecting it in the list and clicking **Modify**.
You can modify the following fields:
 - **Trust Level**

- IP address
- Port
- Key type
- Key value



Tip: You can also change the trust level by selecting a known host key from the list and clicking **Set trust level to Strong** in the toolbar.

- Delete a known host key by selecting it in the list and clicking **Delete**.

Related tasks

[Create or modify an SSH known host key](#) on page 256

Create or modify an SSH known host key

Use the **New/Modify SSH Known Host** window to create or modify SSH known host keys.

Steps

- 1) From the **Trust level** drop-down menu, select **Strong** or **Weak**.



Tip: For option descriptions, click **Help**.

- 2) In the **IP address** field, type the IP address of the host that the new known host key corresponds to.
- 3) If necessary, change the port specified in the **Port** field to match the port that the host's SSH server is listening on.
- 4) From the **Key type** drop-down list, select the appropriate key type.
- 5) Enter the host key data by doing one of the following:
 - Paste the key data in the **Key value** field.
 - Retrieve the key from the remote host by clicking **Retrieve key**.
 - Import the key by clicking **Import from file**, then browsing to the appropriate key file.
- 6) Click **Add**. The window closes and the new host key is added to the list of host keys.

Result



Note: When a user connects to an SSH server through the firewall and accepts a host key, the key added to the SSH Known Hosts list. Accepted keys automatically have a weak trust level.

Related concepts

[Understanding the SSH known host keys trust relationship](#) on page 252

Deny access based on country of origin

Use Geo-Location network objects in access control rules to match country of origin.

Scenario:

Assume that your organization needs to prevent users in Iran from accessing a download server to comply with export controls.

To deny all inbound connections from Iran, perform the following tasks.

Create a Geo-Location network object

Create a Geo-Location network object that contains Iran.

Steps

- 1) Select **Policy > Network Objects**.
- 2) Click **New > Geo-Location**.
- 3) In the **Name** field, type `Iran`.



Tip: For option descriptions, click **Help**.

- 4) In the **Available members** list, double-click **Iran, Islamic Republic of**. Iran moves to the **Chosen Members** list.
- 5) Click **OK**.
- 6) Save your changes.

Create a deny access control rule

Create an access control rule to deny inbound connections from Iran.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.
- 3) In the **Name** field, type `Deny Iran`.

4) Make the following selections.

Option	Selection
Action	Deny
Applications	<Any>
[Source] Zone	external
[Source] Endpoints	Iran (Geo-Location)
[Destination] Zone	external

5) Click OK.

6) Position the new access control rule so that it is above all inbound redirect rules.

7) Save your changes.

Deny access to an application category

Sidewinder allows you to deny access to all applications that belong to an application category. You can also exempt specific users by creating access control rules that allow access for them.

Scenario:

Assume that you want to:

- Allow all users to access the web.
- Prevent most users from using social network applications.
- Allow the Marketing group to use Facebook to promote your organization.

Configuration prerequisites:

- Passive identity validation must be configured on your firewall.
- An access control rule must be in place to allow outbound HTTP.



Note: If your configuration does not match these assumptions, refer to the related topics below.

In this scenario, three access control rules are required.

Table 62: Required access control rules

Rule position	Application	Action	Users and Groups
<i>n</i>	facebook	Allow	Marketing group
<i>n+1</i>	<Social Networking> (Filter)	Deny	None specified (matches all users)
<i>n+2</i>	HTTP	Allow	None specified (matches all users)

To configure this scenario, perform the following tasks.

Related concepts[Passive identity validation](#) on page 94**Related tasks**[Create an access control rule](#) on page 203

Deny access to social networking applications

Create an access control rule that denies access to social networking applications.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.
- 3) In the **Name** field, type `Deny Social Networking`.
- 4) From the **Action** drop-down list, select **Deny**.
- 5) In the **Applications** pane, select **<Social Networking> (Filter)**.



Tip: For option descriptions, click **Help**.

- 6) Click **OK**. The **Rule Properties** window closes.
- 7) Position the new access control rule so that:
 - It is above your general allow HTTP rule.
 - It is below any rules that allow specific social networking applications.
- 8) Save your changes.



Tip: To find the application category filters more quickly, search for the term **filter**.

Create an exemption for the Marketing group

To allow the Marketing group to use Facebook, create an allow rule and place it above the Deny Social Networking rule.

Steps

- 1) Select **Policy > Access Control Rules**.

- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type `Allow Facebook for Marketing`.
- 4) From the **Action** drop-down list, select **Allow**.
- 5) In the **Applications** pane, select **facebook**.
- 6) In the **Users and Groups** pane, select the **Marketing** group.
- 7) Click **OK**. The **Rule Properties** window closes.
- 8) Position the new access control rule so that it is above the above the **Deny Social Networking** rule.
- 9) Save your changes.

Discovering which applications are in use in a zone

Sidewinder allows you to identify which applications are in use in a zone. When application discovery is enabled for a zone, the firewall identifies the application for each connection that is allowed from that zone.

For example, if an access control rule allows HTTP from the internal zone to reach the Internet, each application allowed by the rule is identified. The application information is audited for further analysis in the Admin Console or other syslog analysis services.

The types of applications allowed from the zone determine which types of applications can be identified.

Table 63: Discovery and example access control rules

Access control rule application	Discovery identifies...
HTTP	HTTP-based applications
SSL/TLS	SSL-encapsulated applications (if decrypted by an SSL rule)
TCP/UDP	TCP- and UDP-based applications
<Any>	All applications

Enable discovery for the source zone

Enable application discovery for the internal zone.

Steps

- 1) Select **Network > Zone Configuration**.
- 2) In the upper pane, select **internal**.



Tip: For option descriptions, click **Help**.

- 3) In the lower pane, select **Application discovery**.
- 4) Save your changes.

Creating an access control rule

All applications that are allowed from the discovery zone are identified. You can employ either of the following strategies when you create access control rules for discovery.

- Identify applications that are already flowing through your access control rules.
- Create access control rules that are intentionally permissive in order to allow many applications and identify them.

Viewing application discovery data

You can view which applications are in use in the following tools.

- **Admin Console Dashboard**
- **Applications area (Policy > Rule Elements > Applications)**
- **Admin Console Audit Viewing area (Monitor > Audit Viewing)**

Related concepts

[Applications](#) on page 70

[Viewing audit data](#) on page 289

Related tasks

[Use the dashboard](#) on page 280

Examine your policy using the Firewall Policy Report

You can open a report in a web browser showing comprehensive details of your Sidewinder policy.

Steps

- 1) Select **Monitor > Firewall Policy Report**.
- 2) Click the **Firewall Policy Report** link to open the report in a web browser.



Tip: For option descriptions, click **Help**.

Inspect and control inbound HTTPS

To inspect and control HTTPS and other SSL-encapsulated applications, the firewall must decrypt SSL connections.

Scenario:

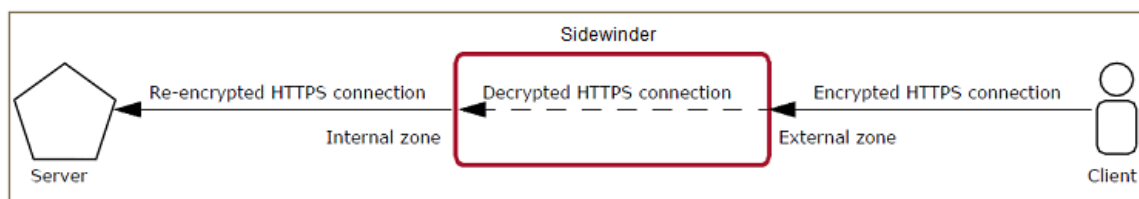
Assume that you want to inspect HTTPS connections from the Internet before allowing them to reach an internal web server. To inspect inbound HTTPS, you can create two types of inbound SSL rules:

- Decrypt only
- Decrypt/re-encrypt

For this example, assume that your organization is required to protect customer information at all times. Therefore, an inbound Decrypt/re-encrypt SSL rule is most appropriate.

Decrypt/re-encrypt SSL rules decrypt matching connections to perform SSL content inspection. Before the connection leaves the firewall, it is re-encrypted. In the figure below, an external client connects to the firewall external IP address and is redirected to an internal server. The firewall decrypts the connection, inspects it, re-encrypts it, then redirects the encrypted connection to the server.

Figure 39: Inbound connection with decryption and re-encryption



To configure this scenario, perform the following tasks.

Configure inbound HTTPS content inspection

Configure inbound HTTPS content inspection. Perform these tasks.

Configuring a CA-signed firewall certificate

When inbound HTTPS inspection is configured, the firewall presents a certificate to clients on behalf of the internal server. This certificate must be signed by an Internet Certificate Authority (CA) that is trusted by internet clients.

To configure a CA-signed firewall certificate, work with the CA of your choice and refer to the related topics below.

Related concepts

[Managing firewall certificates](#) on page 620

Related tasks

[Load manually signed certificates](#) on page 627

Related information

[Managing certificates](#) on page 617

Create an inbound SSL rule

Create an SSL rule to decrypt and re-encrypt inbound SSL connections.

Steps

- 1) Select **Policy > SSL Rules**.
- 2) Click **New Rule**. The **SSL Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type `Inspect inbound SSL`.
- 4) Make the following selections.

Option	Selection
Type	Inbound
Action	Decrypt/re-encrypt
Ports	443
[Source] Zones	external
[Destination] Zones	external

- 5) On the SSL decryption settings tab, select the CA-signed firewall certificate that you configured.
 - If the certificate uses RSA keys, select it from the **RSA** drop-down list, then select **<None>** from the **DSA** drop-down list.
 - If the certificate uses DSA keys, select it from the **DSA** drop-down list, then select **<None>** from the **RSA** drop-down list.

- If you configured RSA and DSA certificates, you can select them both.
- 6) Click **OK**.
 - 7) Position the new SSL rule so that it is above the **Exempt All** rule.
 - 8) Save your changes.

Create access control rules to control inbound HTTPS

If an inbound SSL decryption rule is in place, you can use access control rules to allow and deny most applications that use SSL if they include SSL ports (*SSL/nn*).

Scenarios:

Inspect HTTP/HTTPS and deny other SSL on port 443 for inbound connections

Create an access control rule for the HTTP application.

Assume that you want to:

- Allow inspected inbound HTTP and HTTPS connections.
- Deny other inbound applications that are using SSL on port 443.

To configure this scenario, create an inbound redirect access control rule for the HTTP application.



Tip: Because the HTTP application includes port SSL/443, it matches decrypted HTTPS in addition to normal HTTP connections.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type `Inbound HTTP and HTTPS`.

- 4) Make the following selections.

Option	Selection
Action	HTTP Allow
Applications	HTTP
[Source] Zone	external
[Destination] Endpoints	Firewall external IP
[Destination] Zone	external
NAT	<None>
Redirect	Internal web server

- 5) Click OK.
- 6) Position the new access control rule above the **Deny All** rule.
- 7) Save your changes.

Allow inbound decrypted HTTPS only

Assume that your internal server only accepts HTTPS connections. Therefore, the access control rule should match only HTTPS connections and exclude HTTP connections.

To create the access control rule:

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type **Inbound HTTPS only**.
- 4) Make the following selections.

Option	Selection
Action	Allow
Applications	HTTP
[Source] Zone	external
[Destination] Endpoints	Firewall external IP
[Destination] Zone	external
NAT	None
Redirect	Internal web server

- 5) To prevent the rule from allowing HTTP connections on port 80, override the application ports.
 - a) From the ports drop-down list, select **Override ports**.
 - b) Clear the text box, then type `SSL/443`.
- 6) Click **OK**.
- 7) Position the new access control rule above the **Deny All** rule.
- 8) Save your changes.

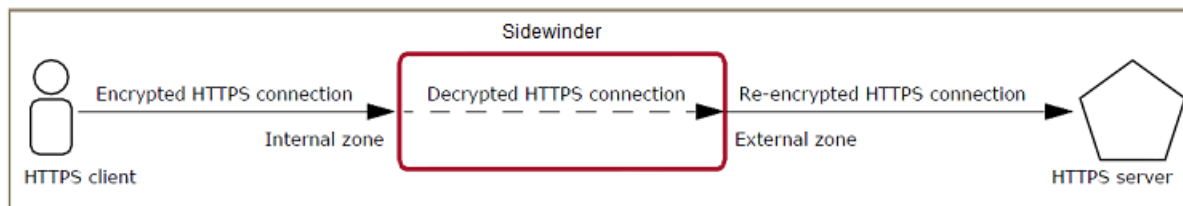
Inspect and control outbound SSL (including HTTPS)

To inspect and control SSL, including HTTPS and other SSL-encapsulated applications, the firewall must decrypt SSL connections.

Scenario:

Assume that you want to inspect SSL connections from internal clients to the Internet. In the figure below, an internal client connects to an external server. The firewall decrypts the connection, inspects it, re-encrypts it, then forwards the encrypted connection to the server.

Figure 40: Outbound decrypt/re-encrypt connection



To configure this scenario, perform the following tasks.

Configure outbound SSL content inspection

To enable outbound SSL content inspection, create an outbound decrypt/re-encrypt SSL rule.

Export the firewall CA certificate to protected clients

The firewall CA signs the surrogate server certificates that are presented to clients. To avoid certificate errors, export the certificate for the firewall CA and install it on the client systems.

Steps

1) Select **Maintenance > Certificate/Key Management**.

2) Click the **Certificate Authorities** tab.



Tip: For option descriptions, click **Help**.

3) In the **Cert Authorities** list, select **Default_SSL_CA**.

4) Click **Export**.

5) Specify a save location, then click **OK**.

6) Install the certificate on all client computers.

Create an outbound SSL rule

Create an SSL rule to decrypt and re-encrypt outbound SSL connections.

Steps

1) Select **Policy > SSL Rules**.

2) Click **New Rule**. The **SSL Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

3) In the **Name** field, type `Decrypt outbound SSL on 443`.

- 4) Make the following selections.

Option	Selection
Type	Outbound
Action	Decrypt/re-encrypt
Ports	443
[Source] Zones	internal
[Destination] Zones	external

- 5) Click OK.
- 6) Arrange the new SSL rule so that it is above the **Exempt All** rule.
- 7) Save your changes.

Create access control rules to control outbound HTTPS and SSL

If SSL content inspection is configured, access control rules can allow and deny most applications that use SSL if they include SSL ports (SSL/nn).

Scenarios:

Inspect HTTP/HTTPS and deny other SSL on port 443 for outbound connections

Configure the required access control rules for the application.

Assume that you want to:

- Allow inspected outbound HTTP and HTTPS connections.
- Deny other applications that are using SSL.

To do so, create two access rules:

Table 64: Required access control rules

Rule position	Application	Action	Source zone	Destination zone
<i>n</i>	HTTP (matches HTTP and decrypted HTTPS)	Allow	internal	external
<i>n+1</i>	SSL/TLS (Matches SSL)	Deny	internal	external

Steps

1) Select **Policy > Access Control Rules**.

2) Create a rule to allow outbound HTTP.



Tip: For option descriptions, click **Help**.

3) Create a rule to deny outbound SSL/TLS.

4) Arrange the new rules so that the allow HTTP rule is positioned before the deny SSL/TLS rule.

5) Save your changes.

Allow outbound decrypted HTTPS only

Assume that you want to allow outbound HTTPS only. To do so, create an access control rule with overridden HTTP ports.

Steps

1) Select **Policy > Access Control Rules**.

2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

3) In the **Name** field, type **Outbound HTTPS only**.

4) Make the following selections.

Option	Selection
Action	Allow
Applications	HTTP
[Source] Zone	internal
[Destination] Zone	external

5) To prevent the rule from matching HTTP connections on port 80, override the application ports.

a) From the ports drop-down list, select **Override ports**.

b) Clear the text box, then type **SSL/443**.

6) Click **OK**.

7) Position the new access control rule above the **Deny All** rule.

8) Save your changes.

Deny Facebook over SSL

Create a deny access control rule that uses the facebook application with overridden ports to deny Facebook over SSL.

Assume that:

- You want to deny SSL connections to Facebook (HTTPS).
- You want to allow unencrypted HTTP connections to Facebook.
- An access control rule is already in place to allow outbound HTTP.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type `Deny Facebook SSL`.
- 4) Make the following selections.

Option	Selection
Action	Deny
Applications	facebook
[Source] Zone	internal
[Destination] Zone	external


- 5) To prevent the rule from blocking access to Facebook over HTTP, override the application ports to remove TCP/80.
 - a) From the ports drop-down list, select **Override ports**.
 - b) Clear the text box, then type `SSL/443`.
- 6) Click **OK**.
- 7) Position the new access control rule above the outbound HTTP rule.
- 8) Save your changes.

Create a rule to allow traceroute through the firewall

To perform a traceroute through the firewall, you must create an application defense and an access control rule.

Steps

- 1) Create a Generic application defense profile.
 - a) Select **Policy > Application Defenses > Defenses > Generic (Required)**.

 **Tip:** For option descriptions, click **Help**.
 - b) Click **New**. A pop-up window appears.
 - c) Type a name for the new profile, then click **OK**.
 - d) Confirm that the new profile is selected, then verify on the **General** tab, that **Use TCP proxy**, **Use UDP proxy**, and **Use ICMP proxy** are deselected.
 - e) On the **Stateful Inspection** tab, select **timxceed_hoplimit**, **timxceed_intrans**, and **unreach_destport**.
 - f) Save your changes.
- 2) Create an application defense group.
 - a) Select **Policy > Application Defenses > Groups**.
 - b) In the upper pane, click **New**. The **New Groups Application Defense** window appears.
 - c) Type a name for the Application Defense group, then click **OK**. The Application Defense group appears in the list in the upper pane.
 - d) In the lower pane, type a description for the Application Defense group.
 - e) In the lower pane on the **Generic (Required)** application defense drop-down list, select the Application Defense profile you created in the previous step.
 - f) Save your changes.
- 3) If you are using UDP, create a custom application.
 - a) Select **Policy > Rule Elements > Applications**.
 - b) Click **New**. The **New Application** window appears.
 - c) In the **Name** field, type a name for the application.
 - d) In the Parent application area, select **TCP/UDP**.
 - e) In the **UDP ports** field, type in the specific ports needed.

- f) Click **OK**.
- 4) Configure the access control rule.
 - a) Select **Policy > Access Control Rules**.
 - b) Click **New > New Rule**. The **Rule Properties** window appears.
 - c) In the **Name** field, type in a name for the rule, such as `Allow Traceroute`.
 - d) In the **Browse** drop-down menu, select **Application defense group**.
 - e) Select the application defense group you created in step 2.
 - f) In the **Browse** drop-down menu, select **Applications**.
 - g) Select **ICMP** and, if needed, the custom application you created in step 3.
 - h) Configure the zones and endpoints as needed.
 - i) Click **OK**.
 - j) Position the rule as needed.
 - k) Save your changes.

Result

You can now run traceroute through the firewall.

Create a SPAN policy

Creating rules for a SPAN interface is similar to creating rules for a standard interface, with a few exceptions.

- Place all SPAN rules at the top of your policy.
- If no rules match SPAN traffic, that traffic will be dropped without any auditing. To avoid this, create an *any-any* SPAN rule.
- Service-specific Application Defenses are not supported. In any SPAN rule, use the **connection settings** Application Defense group or another group that does not have **Use TCP proxy**, **Use UCP proxy**, or **Use ICMP proxy** selected in the **Generic (Required)** defense.
- The following rule configurations are not supported for SPAN rules:
 - IPS
 - NAT
 - Redirect
 - Global Threat Intelligence reputation
 - SSL rules

Related concepts[SPAN interfaces](#) on page 376

Create a SPAN rule

Create a rule for a SPAN interface.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type a name for the rule.
- 4) From the **Action** drop-down list, select the action as appropriate.



Note: Avoid using **Deny** as the action.

- 5) In the **Applications** pane, select the applications as appropriate.
- 6) In the **Source** area, specify the connection sources to match.
 - a) In the **Endpoints** pane, select the endpoints as appropriate.
 - b) From the **Zone** drop-down list, select the zones used by the SPAN interface.
- 7) In the **Destination** area, specify the connection destinations to match.
 - a) In the **Endpoints** pane, select the endpoints as appropriate.
 - b) From the **Zone** drop-down list, select the zones used by the SPAN interface.



Note: The source and destination zones must match. Avoid selecting **<Any>** for either the source or destination zones, as this rule might catch traffic meant for any subsequent rules in the access control rule list.

- 8) From the **Application defense group** drop-down list, select **connection settings**, or another group that does not have **Use TCP proxy**, **Use UCP proxy**, or **Use ICMP proxy** selected in the **Generic (Required)** defense.
- 9) Click **OK**.

- 10) In the **Access Control Rules** window, select the rule and drag it above any non-SPAN rules.



Note: If **<Any>** was selected for either the source or destination zones, place your firewall administrative rules above this rule.

- 11) Save your changes.

Create an any-any SPAN rule

When the firewall receives a connection on a SPAN port it has no rule for, it drops the packet without generating any audit. To verify that the firewall audits all SPAN traffic, create an any-any SPAN rule.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New > New Rule**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type a name for the rule.
- 4) From the **Action** drop-down list, select **Allow**.
- 5) In the **Applications** pane, select **<Any>**.
- 6) In the **Source** area, specify the connection sources to match.
 - a) In the **Endpoints** pane, select **<Any>**.
 - b) From the **Zone** drop-down list, select the zones used by the SPAN interface.
- 7) In the **Destination** area, specify the connection destinations to match.
 - a) In the **Endpoints** pane, select **<Any>**.
 - b) From the **Zone** drop-down list, select the zones used by the SPAN interface.



Note: The source and destination zones must match. Do not select **<Any>** for either the source or destination zones, as this rule would catch traffic meant for all subsequent rules in the access control rule list.

- 8) From the **Application defense group** drop-down list, select **connection settings**, or another group that does not have **Use TCP proxy**, **Use UCP proxy**, or **Use ICMP proxy** selected in the **Generic (Required) defense**.
- 9) Click **OK**.

- 10) In the **Access Control Rules** window, select the rule and drag it to the necessary position.
 - The any-any SPAN rule must be placed after all other SPAN rules for that interface.
 - The any-any SPAN rule must be placed before any non-SPAN rules.

- 11) Save your changes.

PART III

Monitoring

Contents

- [Dashboard](#) on page 279
- [Auditing](#) on page 283
- [Audit responses](#) on page 317
- [McAfee ePolicy Orchestrator integration](#) on page 331
- [Network defenses](#) on page 335
- [SNMP](#) on page 345

View and identify events and responses on managed firewalls.

Dashboard

Contents

- [What the dashboard monitors](#) on page 279
- [Use the dashboard](#) on page 280

The dashboard gives you an overall picture of the system status, resources, messages, and updates. It also allows to view usage reports.

What the dashboard monitors

Use the dashboard to monitor system status, system resources, messages from Forcepoint, updates and usage reports.

- **System status** — The upper left pane displays information about firewall elements. Clicking the links opens windows to view or manage elements.
- **System resources** — This pane displays percentage of use by:
 - Partitions
 - Memory and CPU usage
 - Load average
- **Messages from Forcepoint** — This pane displays information about updates and other product-related announcements.
- **Updates** — The Download updates pane allows manual updates for these services:
 - Virus scanning signatures
 - Application signatures
 - Geo-Location database
 - IPS signatures
 - Messages from Forcepoint
 - SmartFilter database
- **Usage reports** — Tabs in the lower pane display selected audit information about this usage:
 - Applications
 - Threats
 - Policy
 - Geo-Location
 - Users
 - Global Threat Intelligence
 - McAfee EIA

When you log on to the Admin Console, the dashboard appears. To view the dashboard at any time while logged on, select the root node of the tree labeled *firewall_name* **Dashboard**.





Tip: For option descriptions, click **Help**.

Use the dashboard

You can use the dashboard to perform several monitoring and maintenance tasks.

Table 65: Dashboard tasks

Task	Steps
End an Admin Console session for a firewall	In the left tree, select the firewall icon, then click Disconnect .
Maximize or minimize the usage reports display	Click the <i>Toggle usage reports</i> button to maximize or minimize the usage tabs.
Refresh the dashboard information	From the Refresh Rate drop-down list, select how often the dashboard will refresh. The change will not take effect until the next scheduled refresh time. To make the change take effect immediately, click Refresh Now .
Change the firewall host name	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">  Note: Changing the host name affects your DNS configuration, sendmail configuration, and all entries in your <code>/etc/resolv.conf*</code> files. You must manually change any necessary entries to ensure proper functioning. </div> <ol style="list-style-type: none"> 1) In the top of the upper left pane, click the firewall host name link. 2) In the Set Hostname window, modify the host name, then click OK. <p>You will be prompted to restart the firewall. The firewall must be restarted for the change to take effect.</p>
Manually update selected content	<p>In the Download updates pane, select the service you want to update and click Perform update(s)</p> <ul style="list-style-type: none"> • To select multiple consecutive entries, press the Shift key while selecting the entries. To select multiple non-consecutive entries, press the Ctrl key while selecting the entries. • Configure automatic updates or modify the update source by clicking Download updates.

Task	Steps
<p>View detailed audit information</p> <div data-bbox="196 264 250 317" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="282 264 802 348" style="display: inline-block; vertical-align: middle; background-color: #f0f0f0; padding: 5px; margin-left: 10px;"> <p>Note: Only the audit currently archived on the firewall displays.</p> </div>	<p>Use the usage tabs to view audit information for:</p> <ul style="list-style-type: none"> • Applications • Threats • Policy • Geo-Location • Users • Global Threat Intelligence • McAfee EIA <ol style="list-style-type: none"> 1) In the lower pane, click the usage tab you want information for. 2) Select the line of audit you want information for. 3) Click View Audit. <p>You can view report information about this content using the command line. Type one of these commands:</p> <pre>cf usage type=<usage_type> hours=<hours> cf usage type=<usage_type> days=<days></pre> <p>where <usage_type> is what you want to run the report against. For the list of options, run the command <code>man cf_usage</code>. Traffic-related reports begin with <code>traffic_by</code>, and reports for Global Threat Intelligence begin with <code>gti_by</code>.</p> <p><hours> = 1–24 <days> = 1–180</p>

Contents

- [Importance of auditing](#) on page 283
- [Viewing audit data](#) on page 289
- [Filter audit data](#) on page 296
- [Transferring audit records](#) on page 307
- [Managing log files](#) on page 309
- [Export audit data to syslog servers](#) on page 315

Monitoring, auditing, reporting, and attack and system event responses are closely related pieces of the audit process. They function together to provide you with information about the activity on your firewall.

You can monitor the status of various processes in real time, view stored audit information, generate detailed reports, and have the firewall respond to audit events by alerting administrators and ignoring hosts sending malicious packets.

Importance of auditing

Auditing is one of the most important firewall features. Auditing provides information on what is happening with your system and fulfills compliance regulations.

The firewall generates audit information each time it or any of its services stop or start.

Other relevant audit information includes:

- Identification and authentication attempts' successful and failed
- Network communication, including the presumed addresses of the source and destination subject
- Administrative role transitions (srole)
- Modifications to your security policy or system configuration, including all administrator activity (such as changing the system time)

Because audit records are important, storing them is a high priority. The audit facilities monitor the state of log files to minimize the risk of lost data. Log files are compressed, labeled, and stored on a daily basis, and a new "current" log file is created. Using this mechanism, no audit data is lost during the storage transition.

The logcheck utility monitors the amount of available audit storage space very closely. The rollaudit utility rotates log files as needed. See the logcheck man page for more information.

Related concepts

[Monitoring disk space using cron jobs](#) on page 314

Audit components

There are two main components to the Sidewinder audit process.

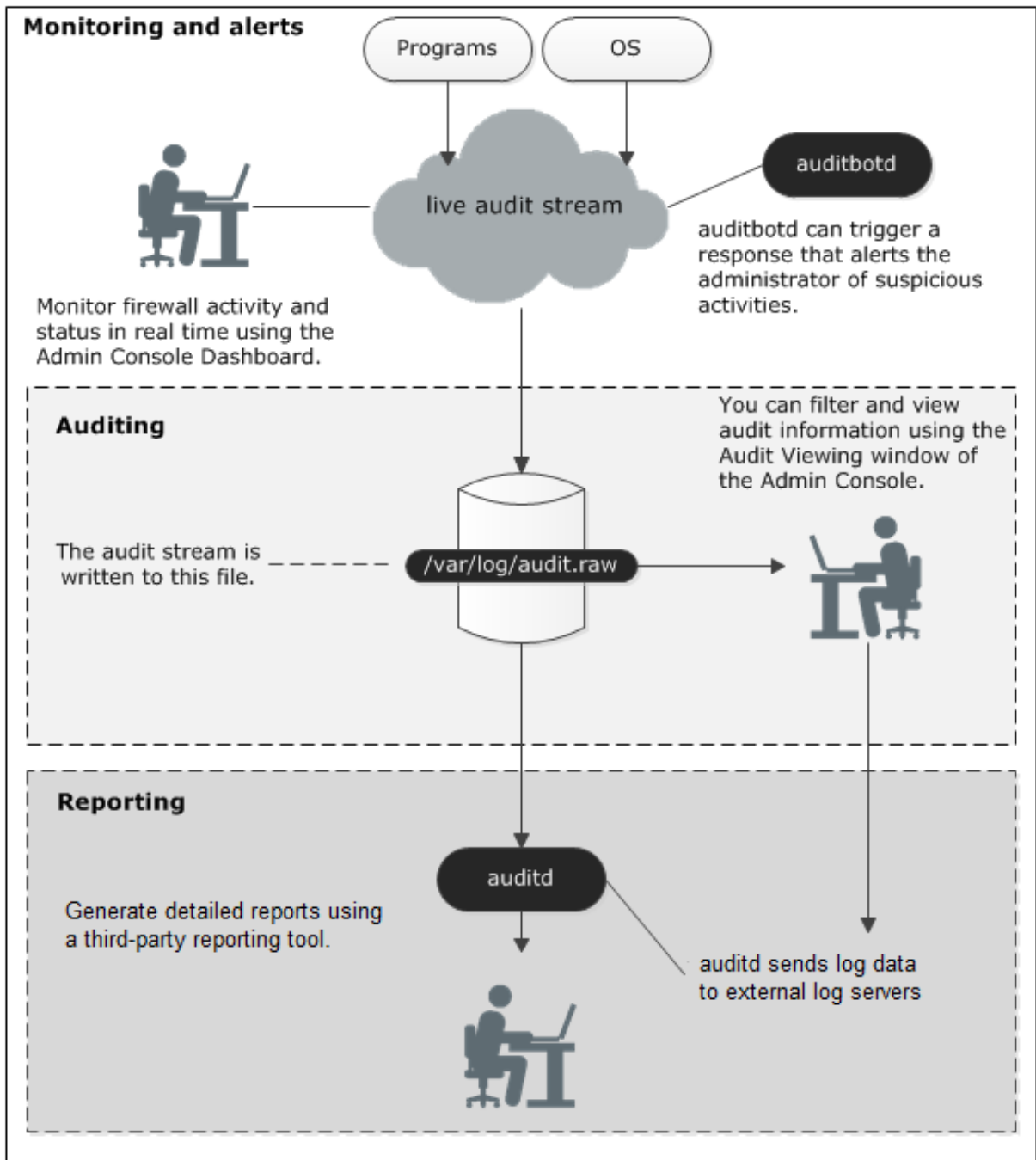
- **auditd** — Audit logging daemon

auditd listens to the firewall audit device and writes the information to log files. The log files provide a complete record of audit events. By default, auditd sends all audit data to a binary file called `/var/log/audit.raw`. auditd can also send log data to external log or syslog servers.

- **auditbotd** — Daemon that listens to the audit device and acts on security-relevant information as configured by the administrator

auditbotd tracks the audit events, then uses its configuration to determine when the data might be indicating a problem that requires a response (such as an attempted break-in). If it detects an audit event that has a configured response, the firewall responds accordingly.

Figure 41: Audit flow



Related information

[Understanding attack and system responses](#) on page 317

Audit file names

Audit information is saved in a binary format in the `/var/log/audit.raw` files. When `rollaudit` rolls the audit file, the file is compressed and a timestamp is included in the file name.

The easiest method for viewing the contents of the `audit.raw` files is to use the **Audit Viewing** window within the Admin Console.

Audit log files are stored in two different formats:

- **Compressed audit data from the interval between the given dates and times (including time zones)** — `audit.raw.YYYYMMDDhhmmssZZZ.YYYYMMDDhhmmssZZZZ.gz`
Example: The `audit.raw.20051231020000CST.20060101020000CST.gz` file contains audit data from December 31, 2005 at 2:00 am CST to January 1, 2006 at 2:00 am CST.
- **Uncompressed audit data** — `audit.raw`

View the audit data from these files using the Admin Console or command line (`acat` or `showaudit`).



Tip: To view the file contents from the command line, refer to the `acat` and `showaudit` man pages.

Related concepts

[Viewing audit data](#) on page 289

Related tasks

[Export or roll log files](#) on page 312

Audit messages

When viewing audit messages, the form of the message will vary depending on the purpose and content of the message.

The form of the first two lines is the same for all audit messages; it provides general information about the process generating or causing the audit. The other lines vary depending on the type of audit message.

Example: Type Enforcement audit message using the `te_filter` filter



Note: Line numbers were added; they correspond to the descriptions in the table.

```
(1) 2010-05-13 08:59:09 -0500 f_kernel a_tepm t_attack p_major
(2) pid: 3747 logid: 101 cmd: "cat" hostname: fw33v190.example.net
(3) category: policy_violation event: ddt violation srcdmn: User
(4) filedom: Admn filetype: diry
(5) reason: OP: OP_FS_PERM_CHECK perm wanted: 0x1 perm granted: 0x0
(6) information: open ssh
```


Table 66: Understanding audit messages




Line number	Contains
1	<ul style="list-style-type: none"> • Date and time • Facility that audited the message (such as Kernel, FTP Proxy, or Telnet Proxy) Examples: kernel, ftp_proxy, telnet_proxy • Location, known as area, in the facility that audited the message (such as general area or type enforcer) Examples: general_area, tepm • Type of audit message (such as attack or network traffic) Examples: attack, nettraffic • Message priority (major or minor) Examples: major, minor
2	<ul style="list-style-type: none"> • Process ID • Log ID • Command associated with the process ID • Firewall host name
3	<ul style="list-style-type: none"> • Audit event category • Audit event • Domain of the requesting process
4	<ul style="list-style-type: none"> • Domain of the file the process is requesting access to • Type of file the process is requesting access to
5 and 6	<ul style="list-style-type: none"> • Reason the audit event was generated • Any additional information

Log file formats

Sidewinder supports several log file formats.

Table 67: Log formats and uses

Log format	Definition
Sidewinder Export Format (SEF)	<p>An ASCII format that can be used to process audit events with a Perl or Python script. SEF is intended for use with reporting tools such as SmartFilter.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Note: If you are using SmartFilter and SEF, set the audit level on the appropriate access control rules (Policy > Access Control Rules) to Verbose.</p> </div>
WebTrends Extended Logging Format (WELF)	An ASCII format used by WebTrends™ reporting tools.

Log format	Definition
W3C Extend Log Format (HTTP)	<p>Specifies HTTP request audit output. This format is intended for tools that understand the W3C format.</p> <p> Note: If you are using this format, set the audit level on the appropriate access control rules (Policy > Access Control Rules) to Verbose.</p>
Extensible Markup Language (XML)	Specifies XML output.
Binary or RAW (bin)	<p>Specifies a raw binary output.</p> <p> Note: Using the <code>acat</code> command is optional; this output is an exact copy of the audit raw file.</p>
American Standard Code of Information Interchange (ascii)	<p>Specifies ASCII output.</p> <p> Note: ASCII is the standard format, so it does not require any arguments with <code>acat</code>.</p>
Verbose American Standard Code of Information Interchange(vascii)	Specifies ASCII output in verbose mode.

Sidewinder syslog server

Sidewinder uses the UNIX syslog facility to log messages sent by programs running on the firewall.

These messages can be useful in detecting unauthorized system users or analyzing hardware or software problems. All syslog data is stored in the audit log files.

Consider these points about syslog and how it works on the firewall:

- syslog runs as a daemon process called *syslogd*.
- Each application determines whether it will use syslog and the types of messages that will be generated. Normally, applications generate messages of different severity levels such as informational and critical.
- Hackers often try to edit syslog files to cover any evidence of their break-ins. The firewall uses Type Enforcement to protect the syslog files from being modified by unauthorized users.
- A copy of the syslog data is sent to the firewall audit log files.
- The log files generated by *syslogd* can become large, using significant hard disk space. To resolve this issue, the log files are periodically rotated.

Related concepts

[System status](#) on page 690

Audit interaction

You can interact with audit data in a variety of ways.

The table lists options for viewing, customizing, and configuring audit output.

Table 68: Audit tools

Option	Definition
Viewing	View audit output using: <ul style="list-style-type: none"> • Admin Console • Audit Viewing window (Monitor > Audit Viewing) • [If change tickets are configured] Configuration Backup window (Maintenance > Configuration Backup)
Customizing	Customize audit output using the Admin Console Network Defenses window (Policy > Network Defenses).
Configuring	Configure audit output to trigger alerts using these Admin Console windows: <ul style="list-style-type: none"> • Attack Responses (Monitor > Attack Responses) • System Responses (Monitor > System Responses)

Related concepts

[Applications](#) on page 70

[Backing up and restoring the firewall configuration](#) on page 606

[Managing attack responses](#) on page 318

[Managing system responses](#) on page 324

Related tasks

[Configure audit options](#) on page 309

Related information

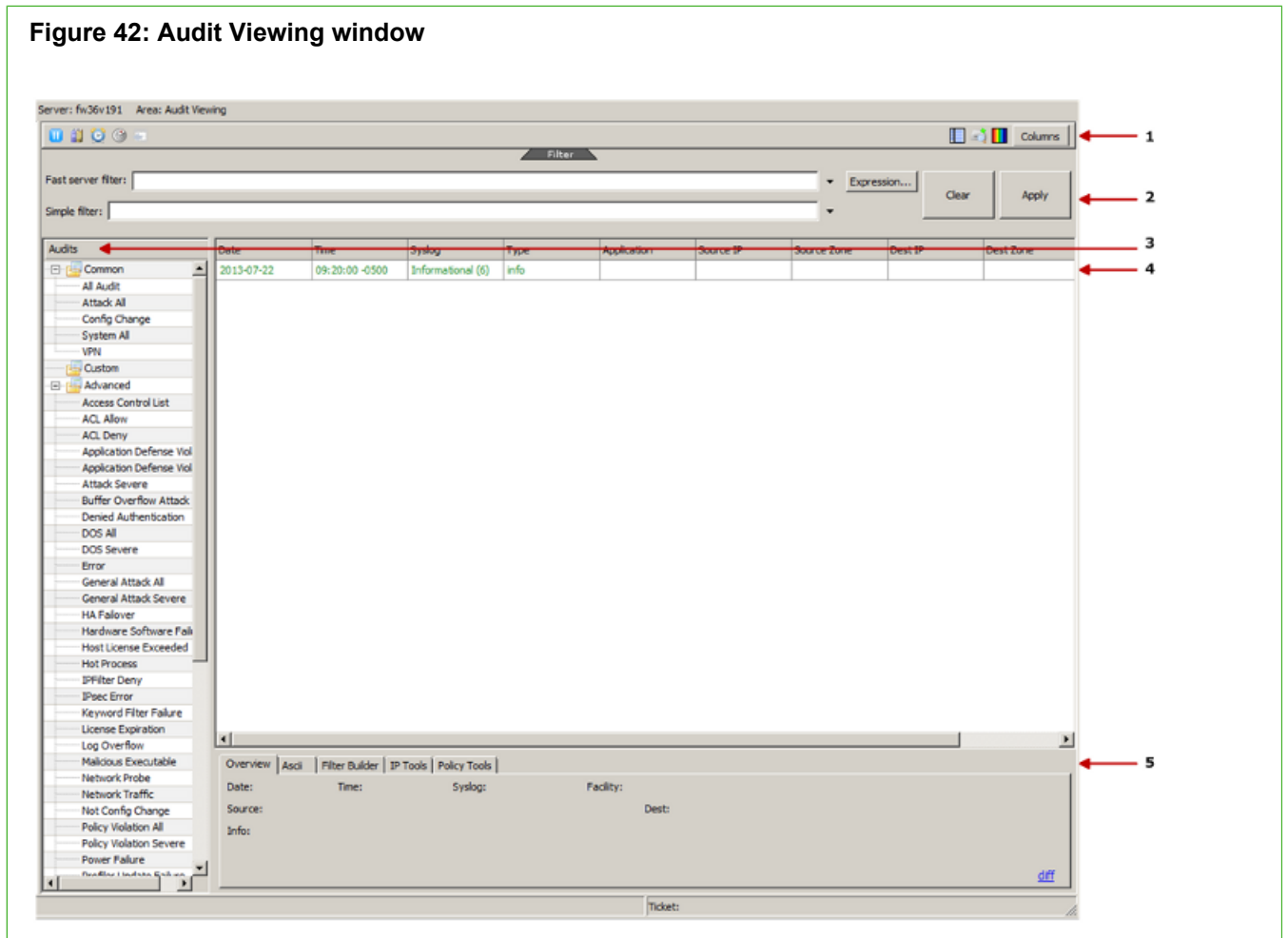
[Viewing network defense information](#) on page 335

Viewing audit data

This section explains the options for viewing audit data.

Select **Monitor > Audit Viewing** to monitor the activity on the firewall. The **Audit Viewing** window appears.

Figure 42: Audit Viewing window



- 1) **Toolbar**
- 2) **Filter shade**
- 3) **Audits pane**
- 4) **Audit records pane**
- 5) **Overview notebook**



Tip: For option descriptions, click **Help**.

The toolbar at the top of the window contains the controls for managing and viewing audit records.

Configure color schemes

You can configure the on-screen color scheme for the audit records. For example, you could use this feature to easily identify types of audit records.

Steps

- 1) From the toolbar, click **Color settings**. The **Color Settings** window appears.



Tip: For option descriptions, click **Help**.

- 2) Select a color scheme:
 - **System colors** — Applies a preset scheme with no color
 - **Minimal color** — Applies a preset scheme with text color
 - **Color** — Applies a preset scheme with background and text color
 - **Custom** — Allows you to modify two of the color schemes
 - Select the **Minimal color** or **Color** scheme.
 - Click the **Background Color** or **Text Color** cell for a severity. The **Color** window appears.
 - Select a color or define a custom color, then click **OK**.
- 3) Click **OK**.

Add or remove columns

Change the data columns that appear in the **audit records** pane.

Steps

- 1) From the toolbar, click **Columns**.
The **Column Selection** window appears.



Tip: For option descriptions, click **Help**.

- 2) Configure the data columns.
 - To add or delete columns:
 - **Add** — Select one or more columns, then click the right arrow.
 - **Delete** — Select one or more columns, then click the left arrow.
 - To change the order of the columns, select a column in the **Show these columns in this order** list, then click **Up** or **Down** to move it to the desired location.
 - To change the columns back to the default firewall format, click **Default**.
- 3) Click **OK**.

Access the Filter shade

The **Filter** shade allows you to access features for applying, creating, and modifying filters.

- Click **Filter** to expand or collapse the **Filter** shade.
- Use the filter fields to find specific audit records
 - **Fast server filter** — SACAP filter
View a selected or modified filter, type a filter, or click the drop-down arrow to select a recently used filter.



Note: Only the Fast server filter can be used with both attack and system responses.

- **Simple filter** — Case-insensitive search of the ASCII records
Type a search string, or click the drop-down arrow to select a recently used search string.



Note: This search is slower because it reads all records. Consider using it to refine the fast server filter search.

- Click **Expression** to access features for creating and modifying filters:
 - Filter builder option
 - Commonly used expressions
 - Advanced options
- Click **Apply** to apply the filter and view matching audit records. Click **Clear** to remove the filter and records from view.

For additional feature descriptions, click **Help**.

Related tasks

[Filter audit data](#) on page 296

Related information

[Understanding attack and system responses](#) on page 317

Access filters in the Audits pane

The **Audits** pane lists predefined common, advanced, and custom filters. Use these filters to view specific audit records.

You can apply or modify common, custom, and advanced filters.



CAUTION: Modifying filters might have unintended effects on Attack or System Responses that reference the filter.

You can also delete custom filters.



Note: Predefined common and advanced filters cannot be deleted.

Click a filter; the filter appears in the **Fast server filter** field in the **Filter** shade. Right-click a filter for additional options.

Related concepts[Audit filters](#) on page 297**Related information**[Understanding attack and system responses](#) on page 317

View data in the audit records pane

The audit records pane displays audit records. Each audit record appears as a single row in the table. See the details for an audit record.

Steps

- 1) Select **Monitor > Audit Viewing**.
- 2) Double-click the audit record. The **Detail View** window appears.



Tip: For option descriptions, click **Help**.

- 3) Use these options to view audit record details; click **Help** for additional descriptions.
 - Click **Field** or **Value** to sort the rows by that column.
 - Right-click a field to access options. To view the man page for the **Cmd** field, right-click **Cmd**, then select **Investigate binary**.
 - Click **Show Details** to see additional fields. Click **Hide Details** to see the default fields again.
 - Click **Copy** to copy the data for transfer to a document or spreadsheet.
 - Click **View Ascii** to view the record in ASCII format.



Tip: You can view multiple records in ASCII format using the **Ascii** tab in the overview notebook.

- Click **Previous** to view the previous audit record; click **Next** to advance to the next audit record.

Related concepts[Transferring audit records](#) on page 307**Related tasks**[View ASCII](#) on page 294

Access the overview notebook

The overview notebook contains a variety of shortcut tools for analyzing and managing audit results. Use the notebook tabs to refine the audit records you want to see.

Compare using overview

The **Overview** tab allows you to see an overview of one or more audit records.

Steps

- 1) Select **Monitor > Audit Viewing**.
- 2) If the overview notebook is not showing, click **Show overview notebook** on the toolbar.



Tip: For option descriptions, click **Help**.

- 3) Select the audit records you want to see data for. The results appear in the **Overview** tab.
 - Bold text highlights matching data.
 - Dashes (--) indicate differences in data.

- 4) For additional details, click **diff**. The **Record Compare** window appears.

This window displays all selected records and compares the audit fields.

- **Similarities** — Cells of the same color indicate matching data.
- **Differences** — Cells in various colors indicate data differences.



Note: The color highlighter differentiates up to five fields of data differences.

- 5) [Optional] To view only similarities or differences, click the drop-down arrow in the **Show** field and make your selection.
- 6) [Optional] Double-click a data field. The **Compare Row** window appears showing the data in column format.
- 7) [Optional] Click **Hide Row** to remove one or more rows from view. Click **Unhide Rows** to display all rows again.

View ASCII

The **Ascii** tab allows you to view audit records in ASCII format.

Steps

- 1) Select **Monitor > Audit Viewing**.
- 2) Select an audit record.



Tip: For option descriptions, click **Help**.

- 3) Click the **Ascii** tab.
If the **Ascii** tab is not visible, click the **Show overview notebook** icon on the toolbar.
- 4) Select one or more records. The selected records appear in ASCII format.



Tip: If you need additional space, copy the records to a document or spreadsheet.

Refine the audit results using Filter Builder

The **Filter Builder** tab (a shortcut to the **Fast server** filter) allows you to refine the audit results.

Steps

- 1) Select **Monitor > Audit Viewing**.
- 2) Click the **Filter Builder** tab.
If the **Filter Builder** tab is not visible, click the **Show overview notebook** icon on the toolbar.



Tip: For option descriptions, click **Help**.

- 3) From the drop-down list, select additional information for the filter, or type the information.
- 4) Select the **And**, **Or**, **And not**, or **Or not** option.



Tip: Use **And not** to find the records you want to see by eliminating the records of no interest.

- 5) Click **Add to Filter**. Only records that match the revised filter remain in the audit records pane.

Diagnose with IP Tools

Use the **IP Tools** tab to perform basic network diagnosis on the IP addresses in your audit.

Steps

- 1) Select **Monitor > Audit Viewing**.
- 2) Select an audit record with a source or destination IP address.



Tip: For option descriptions, click **Help**.

- 3) Click the **IP Tools** tab.
If the **IP Tools** tab is not visible, click the **Show overview notebook** icon on the toolbar.
- 4) In the **IP address** field, click the drop-down arrow to select an IP address:
 - a) **Source IP address**

- b) Destination IP address**
- 5) In the action field, click the drop-down arrow to select the action:
 - **Ping** — Test interface connectivity
 - **Traceroute** — Determine the gateways that traffic passes through
 - **Get route** — Find the first gateway in the route
- 6) Click **Ping**, **Traceroute**, or **Get Route**. The window appears displaying the details.

Create network objects with Policy Tools

The **Policy Tools** tab (a shortcut to **Policy > Rule Elements > Network Objects**) allows you to create an IP network object that you can use later to create policy.

Steps

- 1) Select **Monitor > Audit Viewing**.
- 2) Click the **Policy Tools** tab.
If the **Policy Tools** tab is not visible, click the **Show overview notebook** icon on the toolbar.



Tip: For option descriptions, click **Help**.

- 3) Select a record.
- 4) In the **IP address** field, click the drop-down arrow to select an IP address:
 - **Source IP address**
 - **Destination IP address**
- 5) Click **New IP**. The **IP Address** window appears.
If a network object already exists for this IP address, a notification message appears. Click **Duplicate** to create another network object with this IP address or **Cancel** to cancel the action.
- 6) Complete the information, then click **Add**.

Filter audit data

Audit filters display or exclude certain types of audit records and control the audit data you want to see. Filters can greatly reduce your audit output and simplify troubleshooting.

A high volume of audit records can affect firewall performance. Take these steps to lessen the impact of a large audit record list:

- From the toolbar, click **Pause audit** to temporarily stop records from loading; click **Continue audit** to resume loading records.
- Filter the audit records to reduce the number of records displaying.

Related concepts[Audit filters](#) on page 297**Related tasks**[Manage audit filters](#) on page 303

Audit filters

The firewall includes a variety of predefined filters for your use. The **Audits** pane lists all filters by category.

- **Common** — Predefined common filters
- **Advanced** — Predefined advanced filters
- **Custom** — Filters you created

Common audit filters

The following table lists the predefined common filters and describes the event types that each filter audits.

Table 69: Common filters




Filter	Definition
All Audit	Detects all attack and system events, regardless of characteristics.
Attack All	Detects all severities of Application Defense violation attacks, buffer overflow attacks, DOS attacks, general attacks, policy violation attacks, protocol violation attacks, virus attacks, and spam attacks.
Config Change	Detects when the firewall configuration changes.
System All	Detects all system events of all severities including power failures, hardware and software failures, failover events, license expiration, host license exceeded, log overflows, and IPsec errors.
VPN	Detects VPN audit events.



Advanced audit filters



The following table lists the predefined advanced filters and describes the event types that each filter audits.



Table 70: Advanced filters

Filter	Definition
Access Control List	Detects all ACL audit events.

Filter	Definition
ACL Allow	Detects when a connection is allowed by an access control rule in the active policy.
ACL Deny	Detects when a connection is denied by an access control rule in the active policy.
Application Defense Violation All	Detects attacks of all severities that violate active policy defined by Application Defenses including mime and keyword filter failure attacks.
Application Defense Violation Severe	<p>Detects when severe attacks violate active policy defined by Application Defenses including mime and keyword filter reject audits.</p> <p> Note: Severe attacks indicate something is occurring that an administrator should know.</p>
Attack Severe	<p>Detects severe Application Defense violation attacks, buffer overflow attacks, general attacks, DOS attacks, policy violation attacks, protocol violation attacks, and virus attacks.</p> <p> Note: Severe attacks indicate something is occurring that an administrator should know.</p>
Buffer Overflow Attack	Detects attempted buffer overflow attacks targeted at systems protected by the firewall.
Denied Authentication	<p>Detects when a user attempts to authenticate and types invalid data.</p> <p>For example, if a user is required to type a password and types it incorrectly, the denied auth event logs the event.</p>
DOS All	Detects Denial of Service attacks of all severities; also detects all severities of TCP SYN attacks and proxy flood attacks.
DOS Severe	<p>Detects severe Denial of Service attacks; also detects TCP SYN attacks and proxy flood attacks.</p> <p> Note: Severe attacks indicate something is occurring that an administrator should know.</p>
Error	Detects all system events identified as AUDIT_T_ERROR in the audit stream.
General Attack All	Detects general attacks of all severities that do not fall into the predefined categories.

Filter	Definition
General Attack Severe	<p>Detects severe general attacks that do not fall into the predefined categories.</p> <p> Note: Severe attacks indicate something is occurring that an administrator should know.</p>
HA Failover	Detects when a failover IP address changes because a High Availability cluster failed over to its secondary/standby.
Hardware Software Failure	Detects when a hardware or software component fails.
Host License Exceeded	Detects when the number of hosts protected by the firewall exceeds the number of licensed hosts.
Hot Process	Detects hot process events.
IPFilter Deny	Detects when a connection is denied by the active IP Filter policy.
IPsec Error	Detects when traffic generates IPsec errors.
Keyword Filter Failure	Detects when an SMTP email message is rejected due to a configured keyword filter.
License Expiration	Detects when a licensed feature is about to expire.
Log Overflow	Detects when the log partition is close to filling up.
Malicious Executable	Detects malware executable files sending traffic.
Network Probe	<p>Detects network probe attacks, which occur any time a user attempts to connect or send a message to a TCP or UDP port when there is no access control rule to process traffic on that port.</p> <p> Note: The firewall does not blackhole netprobe attacks as they are likely to be Denial of Service attacks from spoofed source addresses.</p>
Network Traffic	Detects all connections that successfully pass through the firewall.
Not Config Change	Detects all attack and system events that are not configuration changes.
Policy Violation All	Detects attacks of all severities that violate the active policy; also detects all severities of failed authentication attacks, ACL and IP Filter deny attacks, and Type Enforcement error attacks.

Filter	Definition
Policy Violation Severe	<p>Detects severe attacks that violate the active policy; also detects failed authentication attacks, ACL and IP Filter deny attacks, and Type Enforcement error attacks.</p> <p> Note: Severe attacks indicate something is occurring that an administrator should know.</p>
Power Failure	<p>Detects when an Uninterruptible Power Supply (UPS) device detects a power failure and the system is running on UPS battery power.</p>
Protocol Violation All	<p>Detects attacks of all severities that violate protocol compliance.</p>
Protocol Violation Severe	<p>Detects severe attacks that violate proxy protocols (such as HTTP, Telnet, and FTP).</p> <p> Note: Severe attacks indicate something is occurring that an administrator should know.</p>
Proxy Flood	<p>Detects potential connection attack attempts. A connection attack is defined as one or more addresses launching numerous proxy connection attempts to try and flood the system. When NSS receives more connection attempts than it can handle for a proxy, new connections to that proxy are briefly delayed to allow the proxy to "catch up," and the attack is audited.</p>
Signature IPS Intrusion All	<p>Detects all attacks identified by the signature-based IPS.</p> <p>This category detects attacks that were denied, dropped, or rejected as well as suspected attacks that were allowed but were audited by IPS.</p>
Signature IPS Intrusion Blackholed	<p>Detects attacks identified by the signature-based IPS where the attacker was blackholed.</p>
Signature IPS Intrusion Deny	<p>Detects attacks identified by the signature-based IPS where the offending network session was dropped or rejected, or the attacker was blackholed.</p>
Spam	<p>Detects attacks of all severities that are spam.</p>
Spam Severe	<p>Detects severe attacks that are spam.</p>
Syslog	<p>Detects all audit attacks and system events created via syslog.</p>

Filter	Definition
System Critical	<p>Detects critical and severe system events including power failures, hardware failures, critical software failures, and failover events.</p> <p> Note: Critical system events indicate a component or subsystem stopped working; the system is going down (expectedly or unexpectedly), or the system is not expected to work again without intervention.</p>
System Critical and Severe	<p>Detects critical and severe system events including power failures, hardware failures, critical and severe software failures, failover events, license expiration, log overflows, and IPsec errors.</p> <p> Note: Critical system events indicate a component or subsystem stopped working; the system is going down (expectedly or unexpectedly), or the system is not expected to work again without intervention. Severe attacks indicate something is occurring that an administrator should know.</p>
TCP SYN attack	<p>Detects a possible attempt to overrun the firewall with connection attempts.</p>
Type Enforcement	<p>Detects when there is a Type Enforcement violation due to an unauthorized user or process attempting to perform an illegal operation.</p>
Unlisted Executable	<p>Detects unlisted executable files sending traffic.</p>
UPS System Shutdown	<p>Detects when a UPS is running out of battery power or has been on battery power for the estimated battery time.</p>
Virus	<p>Detects attacks of all severities that are viruses.</p>
Virus Severe	<p>Detects severe attacks that are viruses.</p>

Custom audit filters

You can create custom filters for later use. For example, you can modify a predefined common or advanced filter and save that filter as a custom filter.

Filter syntax

Use this syntax when you are building expressions for audit filters.

Table 71: Syntax

Expression	Syntax
"and"	Express using either <code>and</code> or <code>&&</code> .
"not"	Express using either <code>not</code> or <code>!</code> .
"or"	Express using either <code>or</code> or <code> </code> .
() or ("")	Identify a filter using either single quotes (') or double quotes ("). The example in this section uses single quotes.

A filter should include:

- The *type* or *facility* you want to search for using one of these formats:
 - Name format (`AUDIT_T_TYPE` as in `AUDIT_T_ATTACK`, `AUDIT_F_FACILITY` as in `AUDIT_F_LOGIN`)
 - Short Message format (`attack`, `login`)
 - Short Message format prepended with classification indicator (`t_attack`, `f_login`)



Note: This last format appears in audit records and is useful when copying or pasting directly from audit output.

- Additional fields to further specify the audit results

Fields can be separated by Boolean operators (`and`, `or`, `not`) and grouped by parentheses.

Example:

This filter expression:

```
src_ip 10.65.248.154 and dest_zone external
```

returns this audit record:

```
2010-05-13 09:56:46 -0500 f_kernel_ipfilter a_general_area t_nettraffic p_major
hostname: fw1.example.net event: session end app_risk: low
app_categories: infrastructure netsessid: 9f25e4bec131d
srcip: 10.65.248.154 srcport: 1075 srczone: internal protocol: 6
dstip: 10.96.96.120 dstport: 80 dstzone: external
bytes_written_to_client: 729 bytes_written_to_server: 2713
rule_name: Outbound HTTP cache_hit: 0
start_time: 2010-05-13 09:56:29 -0500 application: http
```

The source IP address (10.65.248.154) and destination zone (external) match the filter expression.

Define a time span

View audit records in real time or filter records within a specified time period.

Steps

- 1) From the **Audits** pane, select an audit filter.
- 2) From the toolbar, click **Time Span**. The **Time Span** window appears.



Tip: For option descriptions, click **Help**.

- 3) Select an option.
 - **Real Time** — Select this option to view streaming audit data in real time.
 - **Audit records to display** — From the drop-down list, select the number of records; values range from 10 to unlimited.



CAUTION: Selecting **Unlimited** can impact firewall performance.

- **Sort direction** — From the drop-down list, select the order for displaying audit records.



Note: When you select the **Real Time** option, click **Set as Default** if you want to save your selections as the default settings. This option is not available when you select **Time Period**.

- **Time Period** — Select this option to specify a preset, all-audit, or custom time period. [Conditional] If you selected **Custom**:
 - **Quick Select** — To specify a preset time period, click **Quick Select**, then select a time period.
 - **Custom** — To specify a custom time period, type the dates and times.



Tip: As an alternative, click the drop-down arrows to access the calendar and use the up and down arrows to adjust the time.

Manage audit filters

The firewall includes a variety of predefined audit filters that you can apply and modify to view audit records. You can also create custom filters to meet your needs.

Apply a filter

Apply an existing filter for viewing audit records.

Steps

- 1) If needed, click **Filter** to open the **Filter** shade.



Tip: For option descriptions, click **Help**.

- 2) Select a filter:
 - From the **Audits** pane, select a common, advanced, or custom filter. The filter appears in the **Fast server filter** field.
 - From the **Filter** shade, click the **Fast server filter** drop-down list to select a recently used filter.
- 3) Click **Apply**.
Matching audit records appear in the audit records pane.

Related concepts

[Audit filters](#) on page 297

Create a custom filter from an existing filter

Use an existing filter to create a new custom filter.

Steps

- 1) From the **Audits** pane, locate a filter to create a custom filter from.



Tip: Select a similar filter so you can use the expression as a building block for the new filter.

- 2) Right-click the filter, then select **New filter**. The **New Filter** window appears, and the filter expression appears in the lower pane.



Tip: For option descriptions, click **Help**.

- 3) In the **Name** field, type a name for the filter.



Note: The name cannot be modified.

- 4) [Optional] Type a description to further identify the filter.

- 5) Select a filter type:

- **Attack filter** — Events appear in the **Attack Responses** window.



Tip: The attack filter is a common selection for network-based activity.

- **System filter** — Events appear in the **System Responses** window.

- 6) If you want to send an alert message for an audit event, type the number that corresponds to the trap on your SNMP station. This number is used for the attack or system response.



Note: Refer to the Sidewinder MIB for valid enterprise trap values. Trap numbers in the user interface are based on a value of 200.

Example: To send Attack Trap 202, type 2. If you keep the default value of 0, you are sending User Default Trap 215.

- 7) In the lower pane, update the filter using one or more of these options.

- Type your changes.
- Click **Expression** to select commonly used expressions.
- Click **Expression > Advanced** to access a wider range of filters. The **Filter** window appears. For option descriptions, click **Help**.
- Select a filter from the list. The filter appears in the **Filter Text** field. If **<string>** appears as part of the filter, it indicates that a value is needed. Replace **<string>** with the value.



Tip: Use the **Tab** key to move to the field and automatically select **<string>**.

If the **Filter Text** field appears grayed out, the filter is complete and cannot be edited.

- Click **OK**. The filter appears in the **New Filter** window.
- 8) Click **Validate** to verify that the syntax is correct. If the syntax is incorrect, the invalid portion of the expression appears with a red underline.
 - 9) Click **OK** to save the filter. The filter appears in the **Audits** pane under the Custom category.

Related concepts

[Enabling an SNMP trap](#) on page 329

[SNMP MIBs](#) on page 349

Related tasks

[Build a new custom filter](#) on page 305

Related reference

[Filter syntax](#) on page 302

Related information

[Understanding attack and system responses](#) on page 317

Build a new custom filter

Create a custom filter.

Steps

- 1) If needed, click **Filter** to open the **Filter** shade.
- 2) Click **Expression > Filter builder**. The **Current Filter** window appears.



Tip: For option descriptions, click **Help**.

3) Complete the information for each option you want to include in the filter. The expression builds in the lower pane.

- **Application**
 - [Optional] Type a search string to locate matching applications.
 - Select one or more checkboxes to include the applications in the filter.
- **Source zone** — From the drop-down list, select a zone.
- **Source IP address** — Type an IP address.



Tip: You can also type the number of significant bits needed to create the subnet you want to filter (for example, 192.168.10.0/24).

- **Destination zone** — From the drop-down list, select a zone.
- **Destination IP address** — Type an IP address.



Tip: You can also type the number of significant bits needed to create the subnet you want to filter (for example, 192.168.10.0/24).

- **Ticket ID** — Type the ticket name.

4) Select the **Custom** checkbox. The lower pane becomes active. Continue building the filter using any of these options.

- a) Type additional expressions to include in the filter.
- b) Click **Expression** to select commonly used expressions.
- c) Click **Expression > Advanced** to select from a wider range of filters. The **Filter** window appears.

5) Check the filter for any placeholders that require a value (for example, src_ip a.b.c.d. where *a.b.c.d.* requires a source IP address).

6) Click **Validate** to verify that the syntax is correct. If the syntax is incorrect, the invalid portion of the expression appears with a red underline.

7) [Conditional] If you want to use this filter **one time only** to view matching audit records:

- a) Click **OK**. The filter appears in the **Fast server filter** field.
- b) Click **Apply**.
- c) If the filter contains a syntax error, the **Invalid Filter** window appears. Correct and validate the expression, then click **OK > Apply**.



Note: For option descriptions, click **Help**.

8) [Conditional] If you want to save this filter as a new custom filter:

- a) Select **Save as new filter**. The **New Filter** window appears.

- b) Complete the information, then click **OK > Apply**.

The filter appears in the **Audits** pane under the Custom category, and matching records appear in the audit records pane.



Tip: Use the **Filter Builder** tab in the overview notebook to further refine the audit records you want to see.

Related concepts

[Audit filters](#) on page 297

Related reference

[Filter syntax](#) on page 302

Delete a filter

Delete a custom audit filter.



Note: The predefined common and advanced filters cannot be deleted.

Steps

- 1) Right-click the custom filter you want to delete. The confirmation window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **Yes** to delete the filter or **No** to cancel the action.

Transferring audit records

Copy or export audit records to another location.

Copy audit records

Copy audit data to a document or spreadsheet.

Steps

- 1) From the **audit records** pane, double-click an audit record. The **Detail View** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **Copy**.

3) Select one of these options:

- **As text** — Select this option if you are copying the data to a document.



Tip: If you want to copy multiple records, an easy method is to select the records in the audit records pane. Click the **Ascii** tab, right-click in the **Ascii** pane, and select **Select All**. Paste the text into your document.

- **As table** — Select this option if you are copying the data to a spreadsheet.

4) Paste the data into the document or spreadsheet.

Related tasks

[View ASCII](#) on page 294

[View data in the audit records pane](#) on page 293

Export audit records

Export audit records to another location where you can view, print, or open them in a reporting or editing tool.

Steps

1) Select an option for exporting records.

- **Selected audit records** — To export one or more audit records, select the records in the audit records pane.
- **Time period** — To export audit records created during a specific time period, click Time Span on the toolbar and set the time period.



Note: Exporting all records that match a time period can take a significant amount of time and disk space.

2) From the toolbar, click **Export audit**. The **Export** window appears.



Tip: For option descriptions, click **Help**.

3) Select an option:

- **Selected audit records** — If you chose this option in *Step 1*, select **Export selected audit**.
- **Time period** — If you chose this option in *Step 1*, select **Export all audit in period matching filter**.

4) Select an export format:

- Ascii (Plain Text)
- SEF (Sidewinder Export Format)
- XML

5) Click **Browse**, and navigate to the location you want the export file saved to.

6) Click **Export**. The **Export** window closes and the audit record is saved.

Related tasks[Define a time span](#) on page 303[View data in the audit records pane](#) on page 293

Managing log files

From the **Audit Management** window, you can manage log files.

This includes:

- Export log files in various formats to a specified host
- Schedule exports
- Add a signature to the log files
- Roll the log files
- Identify changes using change tickets

Set up this service during system startup, then test the setup to make sure you are getting the results you intend. Once setup is complete, log files transfer and roll automatically, giving you the audit data you need and keeping the firewall running freely.

Related tasks[Export audit data to syslog servers](#) on page 315

Configure audit options

Audit options include settings to capture changes.

Settings allow you to:

- Capture network and system utilization statistics
- Configure change tickets to track changes made to the firewall

Show system statistics

The firewall captures network and system utilization statistics.



Note: This option should rarely, if ever, need disabling.

Steps

- 1) Select **Monitor > Audit Management**.
- 2) In the **Audit Options** pane, the **Show system statistics in audit log** option is enabled by default.



Tip: For option descriptions, click **Help**.

Use change tickets

You can set up the firewall to require a change ticket when changes are made to the firewall.

Steps

- 1) Select **Monitor > Audit Management**.
- 2) In the **Audit Options** pane, select the **Require change ticket** checkbox.



Tip: For option descriptions, click **Help**.

- 3) Save your change. **Ticket (Required)** appears at the bottom of the window.
- 4) When you make a change to the firewall and click **Save**, the **Change Ticket** window appears.



Tip: You can also manually start a ticket by clicking **Start ticket** on the toolbar.

- a) In the **Ticket** field, type a ticket name.

The name can contain the following:

- 1–32 characters
- Letters, numbers, symbols, underscores, and spaces (quotes, double quotes, and back quotes are not allowed)



Note: If you type an existing ticket name, that ticket will be updated with the new information. If the **Create backups before each change ticket** checkbox is selected, the updated change ticket does not create a new configuration backup.

- b) [Optional] In the **Description** area, type a description of the change you are making to the firewall.
 - c) Click **OK**. The ticket name appears at the bottom of the window.
- 5) The ticket automatically remains open and captures all changes. To close the ticket, click **Stop ticket** on the toolbar.

Create configuration backups

Configure the firewall to automatically create a configuration backup before each change ticket.

Steps

- 1) Select **Monitor > Audit Management**.
- 2) In the **Audit Options** pane, select the **Create backups before each change ticket** checkbox.



Tip: For option descriptions, click **Help**.

- 3) In the **Number of automatic backups to keep** field, type the number.
Before a change ticket is started, the firewall creates a Lite backup. This backup does not include the home directories or support bundle, making it smaller than a full configuration backup.
- 4) To view the audit records for this backup:
 - a) Select **Maintenance > Configuration Backup**.
 - b) In the **Current local configuration backups** pane, select the Lite backup.
 - c) Click **Audit**. The audit records appear.

Related tasks

[View data in the audit records pane](#) on page 293

[Manage configuration backups](#) on page 613

Configure log file options

Log file options include settings for creating and managing export files.

Related concepts

[Monitoring disk space using cron jobs](#) on page 314

Create or modify an export entry

Create a new export entry or modify an existing entry.

Steps

- 1) From the toolbar, click **New** or **Modify**. The **Export File** window appears.



Tip: For option descriptions, click **Help**.

- 2) Add or update the information:
 - **Entry Name** — Type a name for the export entry; the name appears in the **Export Entry** pane.
 - **Export Type** — Select a format for the export entry.
 - **Export with** — From the drop-down list, select the **FTP** or **SCP** transfer protocol.



Note: Forcepoint strongly recommends using the SCP protocol if it is supported by the destination host.

- **Host** — Type the host name or IP address of the host that will receive the exported file.
- **Directory** — Type the directory name where the file will be exported to.
- **Username** — Type the user name for the host you specified.
- **Password** — Type the password for the host you specified.

- 3) Click **OK**.
- 4) If you created a new export entry, test it to make sure the results are what you intended.

Related concepts

[Log file formats](#) on page 287

Delete an export entry

Delete an audit export entry.

Steps

- 1) In the **Export Entry** pane, select the export entry you want to delete.



Tip: For option descriptions, click **Help**.

- 2) From the toolbar, click **Delete**. The confirmation window appears.
- 3) Click **Yes** to delete the entry or **No** to cancel the action.

Sign export files

Log files can be cryptographically signed to ensure data integrity.

Steps

- 1) In the **Signature Options** area, select the **Sign exported files** checkbox.



Tip: For option descriptions, click **Help**.

- 2) Select an option for how you want to store the signature file:
 - **Append signature to exported file** — Creates one `.gz` file that includes the signature at the end of the file
 - **Put signature in separate file** — Creates two files:
 - `.gz` — Contains the actual audit
 - `.gz.pem` — Contains the signature
- 3) In the **Sign with** field, click the drop-down arrow to select the signature certification.

Export or roll log files

When you configure and enable a schedule, the firewall automatically checks to determine whether any log files need to be exported and, if so, exports them.

The firewall automatically rolls log files every morning at 2:00 a.m and maintains a default of 20 rolled instances of the `audit.raw` file. This setting can be reconfigured in the `/etc/sidewinder/rollaudit.conf` file.

You can configure a schedule, or export or roll log files on request.

Configure a schedule to export and roll log files

To set up a schedule for exporting or rolling log files, use the **Crontab Editor** window.

Steps

- 1) In the **Export logfiles** or **Roll logfiles** area, click **Change**. The **Crontab Editor** window appears.



Tip: For option descriptions, click **Help**.

- 2) Select an option for enabling the schedule:

- **Activate** — Select the **Enable** checkbox to activate the schedule.
- **Save, but do not activate** — Deselect the **Enable** checkbox to save the schedule but not have the firewall act on it.

- 3) [Conditional] To designate a standard frequency for exporting files (for example, every day at 2:00 a.m.):

- **Frequency** — From the drop-down list, select the frequency for exporting the file. Based on your selection, add the additional details.



Tip: You can type the time or use the up and down arrows to select it.

- **Hourly** — Minutes after the hour
- **Daily** — Time of day
- **Weekly** — One or more days of the week and time of day

- 4) [Conditional] To define a custom frequency for exporting files:

- a) Select the **Custom** checkbox.

- b) Type the time in the fields.



Tip: Click **Help** for option descriptions, or refer to `man 5 crontab` for options.



Note: The **Crontab Editor** allows custom syntax. Make sure your syntax is correct, and verify your entry with `cf crontab query`.

- 5) [Optional] Add a descriptive name for the task.

Examples:

- Run export utility 35 minutes past every hour
- Run export utility the 1st and 15th day of every month at 2:00 a.m.

- 6) Click **OK**.

Export log files on request

Export all log files from the firewall.

Steps

- 1) [Conditional] If you want to delete log files from the firewall after they are exported, select the **Delete logs after export** checkbox.



Tip: For option descriptions, click **Help**.

- 2) Click **Export All Now**.

Roll log files on request

Rolling log files is generally used for testing and troubleshooting purposes.

To immediately roll all log files, click **Roll Now**.

Monitoring disk space using cron jobs

The roll audit cron job serves an important function in monitoring available disk space.

There are two `rollaudit` jobs.

- The first job checks the size of various audit and log files daily at 2:00 a.m.
- The second job runs each hour and rotates files found to be growing too quickly.

When these jobs run, they check the `/secureos/etc/rollaudit.conf` configuration file to see which files should rotate. The following files are checked by `rollaudit`:

- `/var/log/audit.raw` (The firewall generates reports when these files are rolled.)
- `/var/log/cron`
- `/var/log/daemon.log`
- `/var/log/daemond.log`
- `/var/log/messages`
- `/var/log/maillog` (This file is rotated once a week.)
- `/var/log/SF.log`
- `/var/log/snmpd.log`

You can edit the `/secureos/etc/rollaudit.conf` file to specify how large files can be before they are rotated and the maximum amount of time that should elapse between rotations.

See the `rollaudit` man page for details on editing this file.



CAUTION: To avoid serious system problems, do not allow the `/var/log` partition to become full. Logcheck generates an email alert when `/var/log` becomes 75% full based on the configuration in `/etc/sidewinder/logcheck.conf`. If `/var/log` continues to grow, logcheck generates additional email alerts at every 5% increment (80%, 85%, 90%, 95%, and 100%).

Export audit data to syslog servers

The **Export audit to syslog servers** pane allows you to manage audit data exports to a syslog server. The firewall provides options for converting audit data into various formats used by third-party reporting tools.

Generate reports based on the log files.

Steps

- 1) Select **Monitor > Audit Management**.
- 2) Click the **Syslog** tab.



Tip: For option descriptions, click **Help**.

- 3) Select a format for the audit data.
- 4) Export the formatted files to the computer or host that contains the software for generating log reports.
- 5) Generate the Sidewinder log reports on that computer.

Create a syslog server export entry

Redirect audit output to a syslog server.

Steps

- 1) From the toolbar, click **New**.



Tip: For option descriptions, click **Help**.

- 2) Click the **IP Address** cell, and type the IP address of the syslog server you are sending audit data to.
- 3) From the **Remote Facility** drop-down list, select a syslog facility to help identify the audit export.
- 4) [Optional] Click in the **Description** cell and type a further description of the audit export entry.
- 5) [Optional] If you want to define additional parameters for an export entry, select the entry and click **Advanced**. The **Advanced Syslog Settings** window appears.



Tip: For option descriptions, click **Help**.

- 6) Specify the additional parameters:
 - a) **Port** — The default port is **514**.
 - b) **Filter** — From the drop-down list, select a filter to include or exclude certain types of audit records.
 - c) **Format** — From the drop-down list, select the format to convert the audit data into.

- d) **Max PDU size** — Type the maximum size of the syslog record.
 - e) **PDU exceed behavior** — From the drop-down list, select a method for auditing export records that exceed the maximum PDU size.
- 7) Click **OK**.

Delete a syslog export entry

Delete a syslog server export entry.

Steps

- 1) Select the entry and click **Delete** on the toolbar. The confirmation window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **Yes** to continue or **No** to cancel the action.

Audit responses

Contents

- [Understanding attack and system responses](#) on page 317
- [Managing attack responses](#) on page 318
- [Managing system responses](#) on page 324
- [Ignore network probe attempts](#) on page 328
- [Enabling an SNMP trap](#) on page 329

Sidewinder attack and system event responses allow you to monitor your network for abnormal and potentially threatening activities ranging from an attempted attack to an audit overflow.

Understanding attack and system responses

When the firewall encounters audit activity that matches specific type and frequency criteria, the firewall acts on that activity using the response you configured for that event.

The firewall can respond to events as follows:

- Alert an administrator by email and/or SNMP trap
- Ignore packets from particular hosts for a specific period of time (known as Strikeback™)

You can configure audit output to trigger alerts using attack and system responses. The configuration options you select depend mainly on your site's security policy and, to some extent, your experience using the features. Consider starting with the preconfigured options, then adjust to meet your needs.

Related concepts

[What attack filters detect](#) on page 318

Related tasks

[Filter audit data](#) on page 296

Related reference

[System events](#) on page 324

Managing attack responses

Attack responses allow you to configure how the firewall should respond to audit events that indicate a possible attack (for example, Type Enforcement violations and proxy floods).

This section describes the predefined attack filters and explains how to configure an attack response.




What attack filters detect




An *attack* is generally defined as suspect traffic at either the network or application level.

The firewall includes some predefined attack filters, each detecting a different audit activity. Refer to the table for a description of these filters.

Table 72: Predefined attack filters

Attack filter	Description
ACL Deny	Detects when a connection is denied by an access control rule in the active policy.
Application Defense Violation All	Detects attacks of all severities that violate active policy defined by Application Defenses. This attack category includes mime and keyword filter failure attacks.
Application Defense Violation Severe	Detects when severe attacks violate active policy defined by Application Defenses, including mime and keyword filter reject audits.
Attack All	Detects attack events. <ul style="list-style-type: none"> • Application Defense violation • Buffer overflow • DOS • General • Policy violation • Protocol violation • Spam • Virus

Attack filter	Description
Attack Severe	<p>Detects severe attacks.</p> <div data-bbox="857 262 1468 380" style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-bottom: 10px;">  Note: Severe attacks indicate something is occurring that an administrator should know. </div> <ul style="list-style-type: none"> • Application Defense violation • Buffer overflow • DOS • General • Policy violation • Protocol violation • Spam • Virus
Buffer Overflow Attack	<p>Detects attempted buffer overflow attacks targeted at protected systems.</p>
Denied Authentication	<p>Detects when a user attempts to authenticate and enters invalid data. Example: If a user is required to enter a password and enters it incorrectly, Denied Authentication logs the event.</p>
DOS All	<p>Detects Denial of Service attacks of all severities; also detects all severities of TCP SYN attacks and proxy flood attacks.</p>
DOS Severe	<p>Detects severe Denial of Service attacks; also detects TCPSYN attacks and proxy flood attacks.</p> <div data-bbox="857 1266 1468 1383" style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;">  Note: Severe attacks indicate something is occurring that an administrator should know. </div>
General Attack All	<p>Detects general attacks of all severities that do not fall into the predefined categories.</p>
General Attack Severe	<p>Detects severe general attacks that do not fall into the predefined categories.</p> <div data-bbox="857 1602 1468 1719" style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;">  Note: Severe attacks indicate something is occurring that an administrator should know. </div>
IPFilter Deny	<p>Detects when a connection is denied by an access control rule in the active policy.</p>
Keyword Filter Failure	<p>Detects when an SMTP email message is rejected due to a configured keyword filter.</p>
Malicious Executable	<p>Detects a malware executable file sending traffic.</p>

Attack filter	Description
<p>Network Probe</p>	<p>Detects network probe attacks, which occur any time a user attempts to connect or send a message to a TCP or UDP port that there is no access control rule for.</p> <p> Note: The firewall does not blackhole netprobe attacks as they are likely to be denial of service attacks from spoofed source addresses.</p>
<p>Policy Violation All</p>	<p>Detects attacks of all severities that violate the active policy; also detects all severities of failed authentication attacks, ACL and IP Filter deny attacks, and Type Enforcement error attacks.</p>
<p>Policy Violation Severe</p>	<p>Detects severe attacks that violate the active policy; also detects failed authentication attacks, network probe attacks, ACL and IP Filter deny attacks, and Type Enforcement error attacks.</p> <p> Note: Severe attacks indicate something is occurring that an administrator should know.</p>
<p>Protocol Violation All</p>	<p>Detects attacks of all severities that violate protocol compliance.</p>
<p>Protocol Violation Severe</p>	<p>Detects severe attacks that violate proxy protocols (such as HTTP, Telnet, and FTP).</p> <p> Note: Severe attacks indicate something is occurring that an administrator should know.</p>
<p>Proxy Flood</p>	<p>Detects potential connection attack attempts. A connection attack is defined as one or more addresses launching numerous proxy connection attempts to try and flood the system. When NSS receives more connection attempts than it can handle for a proxy, new connections to that proxy are briefly delayed, allowing the proxy to catch up, and the attack is audited.</p>
<p>Signature IPS Intrusion All</p>	<p>Detects all attacks identified by the signature-based IPS.</p> <p>This category detects attacks that were denied, dropped, or rejected as well as suspected attacks that were allowed but audited by IPS.</p>
<p>Signature IPS Intrusion Blackholed</p>	<p>Detects attacks identified by the signature-based IPS where the attacker was blackholed.</p>

Attack filter	Description
Signature IPS Intrusion Deny	Detects attacks identified by the signature-based IPS where the offending network session was dropped, rejected, or the attacker was blackholed.
Spam	Detects attacks of all severities that are spam.
Spam Severe	Detects severe attacks that are spam.
TCP SYN Attack	Detects a possible attempt to overrun the firewall with connection attempts.
Type Enforcement	Detects when a Type Enforcement violation occurs due to an unauthorized user or process attempting to perform an illegal operation.
Unlisted Executable	Detects when an unlisted executable file sends traffic.
Virus	Detects attacks of all severities that are viruses.
Virus Severe	Detects severe attacks that are viruses.

Related concepts

[Audit filters](#) on page 297

Create an attack response

Use the **Add Attack Response Wizard** to create a new attack response.

Steps

- 1) Select **Monitor > Attack Responses**. The **Attack Responses** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New**. The **Add Attack Response Wizard** appears.

- 3) Click **Next**, and follow the on-screen instructions.

Modify an attack response

Modify an existing attack response.

Steps

- 1) Select **Monitor > Attack Responses**. The **Attack Responses** window appears.



Tip: For option descriptions, click **Help**.

- 2) Select the attack response, then click **Modify**. The **Modify Attack Response** window appears with the **Attack** tab open and the attack response highlighted.
- 3) Make your changes.
 - If you want to enable or disable this attack filter, select or deselect the **Enable** checkbox.
 - If you want to associate a different filter with this attack response, select the attack filter.
- 4) Click the **Attack Frequency** tab.
- 5) Make your changes.
 - Select a frequency.
 - If you selected **Limit Responses**, configure the response settings and Reset option.
- 6) Click the **Attack Response** tab.
- 7) Make your changes.
 - **Alerts** — To send an alert, configure the email and/or SNMP trap settings.
 - **Strikeback** — To use this option, select the **Blackhole** checkbox and configure the settings.
- 8) Click **OK**.

Related concepts

[Enabling an SNMP trap](#) on page 329

[What attack filters detect](#) on page 318

Related tasks

[Configure email settings for an attack response](#) on page 322

[Create a custom filter from an existing filter](#) on page 304

Configure email settings for an attack response

Create, modify, or delete the email notification list for attacks that trigger alerts. You can also blackhole a source IP address if the attack IP cannot be confirmed.



Tip: If you have not already done so, create an off-box alias for the root and administrator email accounts. This ensures that system messages are sent to an account that is checked regularly. If email is not forwarded or checked regularly, the local mailbox could use too much hard disk space and cause problems.

Steps

- 1) From the **Attack Responses** window, click **Response Settings**. The **Response Settings** window appears.



Tip: For option descriptions, click **Help**.

- 2) Use the task table to configure an email group.

Task	Steps
Create an email group	<ol style="list-style-type: none"> 1) Click New. The Email Addresses window appears. 2) In the Group Name field, type a description name for the email group. 3) In the Email Addresses window, type the list of email addresses to include in this group. Use a comma to separate email addresses in the list. 4) Click OK. The group appears on the Response Settings window.
Modify an email group	<ol style="list-style-type: none"> 1) Select the email group, then click Modify. The Email Addresses window appears. 2) Make your changes, then click OK.
Delete an email group	<ol style="list-style-type: none"> 1) Select the email group you want to delete. 2) Click Delete. The confirmation window appears. 3) Click Yes to delete the group or No to cancel the action.

- 3) If you want to blackhole a source IP when the related audit message does not have an **Attack IP** field, select the **Blackhole source IP if attack IP cannot be confirmed** checkbox.
- 4) Click **OK** on the **Response Settings** window.

Related tasks

[Set up email aliases for administrator accounts](#) on page 506

Delete an attack response

Delete an attack response.

Steps

- 1) Select the attack response, then click **Delete**. The confirmation window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **Yes** to delete the response or **No** to cancel the action.

Managing system responses

System responses allow you to configure how the firewall should respond to system audit events (for example, license failures and log overflow issues).

This section describes the predefined system filters and explains how to configure a system response.



System events

An *event* is defined as an important, generally unexpected change in your system.

The firewall includes some predefined system filters, each detecting a different audit activity. Refer to the table for a description of these filters.

Table 73: Predefined system filters

Event	Description
Access Control List	Detects all ACL audit events.
ACL Allow	Detects when a connection is allowed by an access control rule in the active policy.
All Audit	Detects all attack and system events, regardless of characteristics.
Config Change	Detects when the firewall configuration changes.
Error	Detects all system events identified as AUDIT_T_ERROR in the audit stream.
HA Failover	Detects when a failover IP address changes because a High Availability cluster failed over to its secondary or standby.
Hardware Software Failure	Detects when a hardware or software component fails.
Host License Exceeded	Detects when the number of hosts protected by the firewall exceeds the number of licensed hosts.
Hot Process	Detects hot process events.
IPsec Error	Detects when traffic generates IPsec errors.

Event	Description
License Expiration	Detects when a licensed feature is about to expire.
Log Overflow	Detects when the log partition is close to filling up.
Network Traffic	Detects all connections that successfully pass through the firewall.
Not Config Change	Detects all attack and system events that are not configuration changes.
Power Failure	Detects when an Uninterruptible Power Supply (UPS) device detects a power failure and the system is running on UPS battery power.
Syslog	Detects all audit attacks and system events created via syslog.
System All	<p>Detects all system events of all severities, including:</p> <ul style="list-style-type: none"> • Power failures • Hardware and software failures • Failover events • License expiration • Host license exceeded • Log overflows • IPSEC errors
System Critical	<p>Detects all critical system events, including the following:</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin: 10px 0;"> <p> Note: Critical system events indicate that a component or subsystem stopped working, that the system is going down expectedly or unexpectedly, or that the system is not expected to work again without intervention.</p> </div> <ul style="list-style-type: none"> • Power failures • Hardware failures • Critical software failures • Failover events
System Critical And Severe	<p>Detects critical and severe system events, including the following.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin: 10px 0;"> <p> Note: Critical system events indicate a component or subsystem stopped working, that the system is going down expectedly or unexpectedly, or that the system is not expected to work again without intervention. Severe attacks indicate something is occurring that an administrator should know.</p> </div> <ul style="list-style-type: none"> • Power failures • Hardware failures • Critical and severe software failures • Failover events • License expiration • Log overflows • IPSEC errors

Event	Description
UPS System Shutdown	Detects when a UPS is running out of battery power or has been on battery power for the estimated battery time.
VPN	Detects VPN audit events.

Related concepts

[Audit filters](#) on page 297

Create a system response

Use the **Add System Response Wizard** to create a new system response.

Steps

- 1) Select **Monitor > System Responses**. The **System Responses** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New**. The **Add System Response Wizard** appears.
- 3) Click **Next**, and follow the on-screen instructions.

Modify a system response

Modify an existing system response.

Steps

- 1) Select **Monitor > System Responses**. The **System Responses** window appears.



Tip: For option descriptions, click **Help**.

- 2) Select the system response, then click **Modify**.
The **Modify System Response** window appears with the **Event** tab open and the event highlighted.
- 3) Make your changes.
 - If you want to enable or disable this event filter, select or deselect the **Enable** checkbox.
 - If you want to associate a different filter with this response, select the event filter.
- 4) Click the **Event Frequency** tab.
- 5) Make your changes:
 - Select a frequency.
 - If you selected **Limit Responses**, configure the response settings and reset option.

- 6) Click the **Event Response** tab.
- 7) Select the email, SNMP trap, or both options.
If you select **Send SNMP trap**, also configure the time setting.
- 8) Click **OK**.

Related concepts

[Enabling an SNMP trap](#) on page 329
[What attack filters detect](#) on page 318

Related tasks

[Create a custom filter from an existing filter](#) on page 304
[Configure email settings for a system response](#) on page 327

Delete a system response

Delete a system response.

Steps

- 1) Select the response, then click **Delete**. The confirmation window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **Yes** to delete the response or **No** to cancel the action.

Configure email settings for a system response

Create, modify, or delete the email notification list for events that trigger alerts.



Tip: If you have not already done so, create an off-box alias for the root and administrator email accounts. This ensures that system messages are sent to an account that is checked regularly. If email is not forwarded or checked regularly, the local mailbox could use too much hard disk space and cause problems.

Steps

- 1) From the **System Responses** window, click **Response Settings**. The **Response Settings** window appears.



Tip: For option descriptions, click **Help**.

- 2) Use the task table to configure an email group.

Task	Steps
Create an email group	<ol style="list-style-type: none"> 1) Click New. The Email Addresses window appears. 2) In the Group Name field, type a description name for the email group. 3) In the Email Addresses window dialog box, type the list of email addresses to include in this group. Use a comma to separate email addresses in the list. 4) Click OK. The group appears on the Response Settings window.
Modify an email group	<ol style="list-style-type: none"> 1) Select the email group, then click Modify. The Email Addresses window appears. 2) Make your changes, then click OK.
Delete an email group	<ol style="list-style-type: none"> 1) Select the email group you want to delete. 2) Click Delete. The confirmation window appears. 3) Click Yes to delete the group or No to cancel the action.

- 3) Click **OK** on the **Response Settings** window.

Related tasks

[Set up email aliases for administrator accounts](#) on page 506

Ignore network probe attempts

If a host on the network attempts to connect to the firewall for an application that is not running, an audit record is generated that could trigger an alert.

You can set up an ignore list to ignore unimportant network probe audit events but still save the audit to keep track of the probe attempts. To ignore network probes, commonly referred to as *netprobes*, create access control rules that use an application.

Steps

- 1) Create an access control rule with an action of Drop to ignore the connection.



Tip: For option descriptions, click **Help**.

- 2) Select an existing application, or build a custom application to identify the particular ports.



Note: if connection attempts are frequent and are coming from a trusted network, consider configuring filter rules, then ignoring the connection attempts completely and not auditing them.

Related concepts

[Configuring access control rules](#) on page 197

[Custom applications](#) on page 170

Enabling an SNMP trap

An SNMP trap is an unsolicited event notification message sent from a managed node (such as a router or Sidewinder) to a management station.

The firewall provides an option to send audit alert SNMP traps when an audit event, such as an attack or system event, triggers a response.

You can use predefined attack and system filters or create custom traps.

For more information on SNMP traps, see the `snmptrap` man page.

Related concepts

[Audit filters](#) on page 297

[SNMP traps](#) on page 347

Related tasks

[Modify an attack response](#) on page 321

[Modify a system response](#) on page 326

McAfee ePolicy Orchestrator integration

Contents

- [ePolicy Orchestrator and Sidewinder communication](#) on page 331
- [Configure firewalls for ePolicy Orchestrator reporting](#) on page 332
- [Troubleshoot Sidewinder to ePolicy Orchestrator communication](#) on page 333

Administrators can leverage Sidewinder data in McAfee® ePolicy Orchestrator®.

ePolicy Orchestrator is a security management platform that allows organizations to deploy, manage, and integrate products in their security infrastructure.

ePolicy Orchestrator and Sidewinder communication

You can configure transmission of some firewall data from Sidewinder to ePolicy Orchestrator. In ePolicy Orchestrator, you can view the data in the dashboard and run queries on it.

In multiple-firewall network environments, ePolicy Orchestrator enables you to send data for all of your firewalls to a central location. From the data, you can determine whether the firewall software is current and which internal hosts are protected by each firewall. You can also assess the levels of traffic flowing through your network.

The firewall can transmit the following data:

- Protected hosts data
 - IP address of internal hosts passing traffic through the firewall
 - A count of the number of times each IP address is contained in the firewall audit



Note: There can be multiple audit entries for a single connection through the firewall.

- Most recent connection time for each IP address
- Firewall version data
 - Sidewinder version
 - Policy version
 - Signature database versions

The data transmission frequency is as follows:

- **Hourly** — Transmit protected hosts and version data for the previous hour.
- **Every minute** — Transmit new host IP addresses not seen within the previous four hours.

For more information about viewing firewall data in the ePolicy Orchestrator dashboard and running firewall-specific queries, see the *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide*.

Configure firewalls for ePolicy Orchestrator reporting

Configure data transmission from Sidewinder to ePolicy Orchestrator.

Steps

- 1) Set up ePolicy Orchestrator using the getting started instructions in the *McAfee ePolicy Orchestrator Product Guide*.
- 2) Install **Sidewinder ePO Extension 5.2.1** on the ePolicy Orchestrator server using the instructions in the *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide*.
- 3) Set up Sidewinder to transmit data to ePolicy Orchestrator.
 - a) Select **Monitor > ePolicy Orchestrator**. The **ePolicy Orchestrator** window appears.



Tip: For option descriptions, click **Help**.

- b) Complete the following fields to configure the contact information for connections to the ePolicy Orchestrator server:
 - **IP Address** — Type the IP address of the ePolicy Orchestrator server. To find the IP address associated with a host name, use the **DNS Lookup** window.
 - **Port** — Type the ePolicy Orchestrator Client-to-server authentication communication port that ePolicy Orchestrator is listening on for connections. Standard deployments of ePolicy Orchestrator use port 8444.
 - **User name** — Type the user name of an ePolicy Orchestrator user configured on the ePolicy Orchestrator server.
 - **Password** — Type the password of the ePolicy Orchestrator user specified in the **User name** field.
 - **Confirm password** — Type the password again.
 - c) Click **Save**.
 - d) Configure the Certificate Authority (CA) to use for validating the certificate that the ePolicy Orchestrator server presents during a connection.
 - **Self-signed certificate** — If ePolicy Orchestrator uses a self-signed certificate, click **Retrieve ePO root cert** to retrieve the root certificate from the ePolicy Orchestrator server. Then, select **ePO Server Certificate Authority** from the **Cert authority** drop-down list.
 - **CA certificate** — If ePolicy Orchestrator uses a certificate that has been signed by a CA, select the CA from the **Cert authority** drop-down list.
 - e) Click **Save**.
 - f) Select the **Enable communication with ePO** checkbox.
 - g) Click **Save**.

Troubleshoot Sidewinder to ePolicy Orchestrator communication

Perform the following troubleshooting steps if communication is failing from Sidewinder to ePolicy Orchestrator.

Steps

- 1) Make sure you have installed **Sidewinder ePO Extension 5.2.1** on the ePolicy Orchestrator server.
- 2) Make sure the user configured on the ePolicy Orchestrator server has been assigned a permission set with the **Permit data exchange with Sidewinder systems** option selected.
- 3) Verify connectivity from the firewall to the ePolicy Orchestrator server using ping. You can perform a ping in the Sidewinder Admin Console in the **Tools > Ping host** area.

Network defenses

Contents

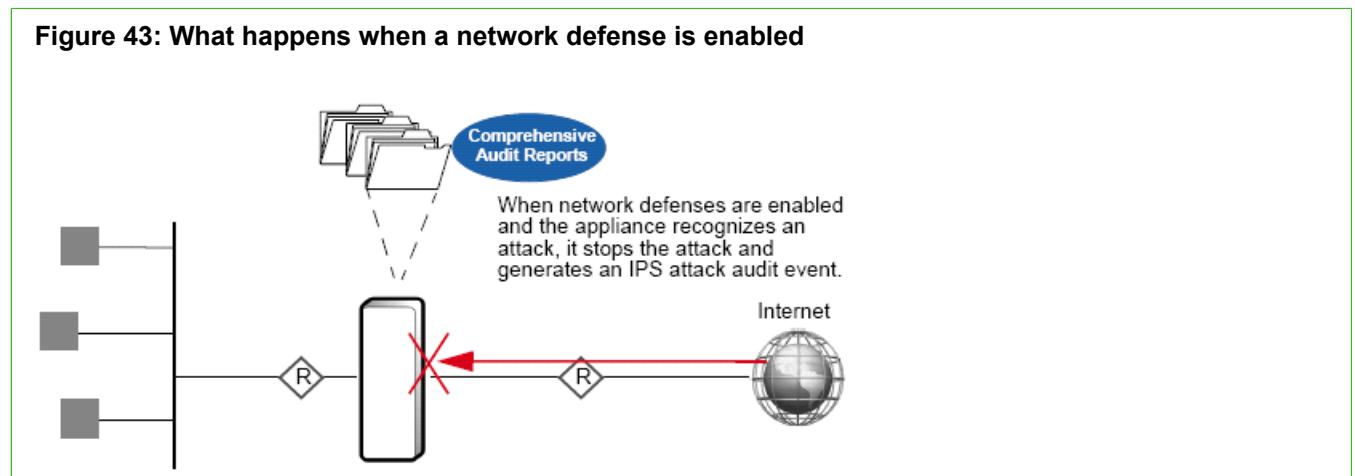
- Viewing network defense information on page 335
- Restore network defenses on page 337
- Configure the TCP network defense on page 337
- Configure the IP network defense on page 338
- Configure the UDP network defense on page 339
- Configure the ICMP network defense on page 339
- Configure the ARP network defense on page 340
- Configure the IPsec network defense on page 341
- Configure the IPv6 network defense on page 342

Network defenses allow you to control the audit output for suspicious traffic at the data link, network, and transport layers that is detected by the Sidewinder when the firewall automatically prevents that traffic from entering the firewall.

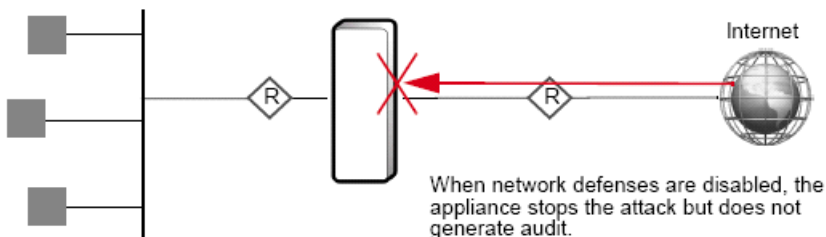
Viewing network defense information

Some traffic is stopped because a packet, or sequence of packets, resembles a known attack. Other traffic is stopped because a packet does not comply with its protocol's standards. If network defenses are enabled, the audit reports provide detailed information on the denied traffic.

Figure 43: What happens when a network defense is enabled



If network defenses are not enabled, the firewall still stops suspicious traffic but does not generate audit.

Figure 44: What happens when a network defense is disabled

Once you decide that you want to view these denied packets' audit, you can configure the following options:

- Audit packets that the firewall determines to be part of an identifiable attack based on attack description (bad header length, bad redirect, etc.).
- Audit packets that are not specifically identified as a potential attack yet are not compliant with their protocol standards at the following levels:
 - All packets that do not comply with their protocol's standards.
 - Packets that do not comply with their protocol's standards and have been identified as a severe or moderate risk to your network.
 - Packets that do not comply with their protocol's standards and have been identified as a severe risk to your network.
 - Do not generate audit when the firewall stops a packet because it does not comply to its protocol's standard.

Network defenses represent one element of the firewall's audit capabilities. Information about additional auditing tools can be found in the following chapters:

- *Dashboard*
- *Auditing*
- *Audit responses*

To view the Network Defenses, select **Policy > Network Defenses**. The **Network Defenses** window displays with the **TCP** tab. All tabs are similar in appearance and function.

The Network Defenses tabs allows you to configure what audit the firewall generates for each of the specified protocols and how frequently to generate that audit.

If you want to return the Network Defense settings to their defaults, click **Restore Defaults**.

Related tasks

- [Configure the TCP network defense on page 337](#)
- [Configure the IP network defense on page 338](#)
- [Configure the UDP network defense on page 339](#)
- [Configure the ICMP network defense on page 339](#)
- [Configure the ARP network defense on page 340](#)
- [Configure the IPsec network defense on page 341](#)

Restore network defenses

Restore the defaults for all or selected network defenses.

- If you want to restore the defaults for all network defenses, click **OK**.
- If you want to restore the defaults for selected network defenses, clear the check box next to the network defenses that need to keep their current settings. After clearing the appropriate check box(es), click **OK**.

The selected network defenses now display and enforce their default settings.

Configure the TCP network defense

The TCP network defense allows you to customize audit output for TCP attacks and compliance issues stopped by the firewall.

Follow these steps to configure the TCP tab.

Steps

- 1) Select **Policy > Network Defenses > TCP**.
- 2) In the **Audit the selected TCP attacks** section, select the attacks for which you want the firewall to generate audit.



Tip: For option descriptions, click **Help**.

- 3) In the **Audit the selected TCP compliance issues** area, select how you want the firewall to audit packets that are not known attacks, but are still not compliant with the TCP standards. Options are:
 - **Audit all TCP compliance issues**
 - **Audit severe and moderate TCP compliance issues**
 - **Audit severe TCP compliance issues**
 - **Do not audit any TCP compliance issues**
- 4) In the **TCP Audit Frequency** area, select how often to generate audit for TCP issues. Select one of the following:
 - **Limit auditing (recommended)** — Generates an audit record for the first x occurrences for every y seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed. For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the firewall stopped 100 SYN-ACK probes in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window. Limiting audit in this manner reduces system load.
 - **Always audit** — Generates an audit record for every audit event.



Note: Unlimited auditing runs the risk of overflowing the log partition and creating problems for the firewall.

Options for viewing the audit output generated by these selections include:

- The Admin Console Dashboard
- **Monitor > Audit**
- Third-party reporting tools

Configure the IP network defense

The IP network defense allows you to customize audit output for IP attacks stopped by the firewall.

Follow these steps to configure the IP tab.

Steps

- 1) Select **Policy > Network Defenses > IP**.
- 2) In the **Audit the selected IP attacks** section, select the attacks for which you want the firewall to generate audit.



Tip: For option descriptions, click **Help**.

- 3) In the **Audit the selected IP compliance issues** area, select how you want to audit packets that are not known attacks, but are still not compliant with the IP standards. Options are:
 - **Audit all IP compliance issues**
 - **Audit severe and moderate IP compliance issues**
 - **Audit severe IP compliance issues**
 - **Do not audit any IP compliance issues**
- 4) In the **IP Audit Frequency** area, select how often to generate audit for IP issues. Select one of the following:
 - **Limit auditing (recommended)** — Generates an audit record for the first *x* occurrences for every *y* seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed. For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the firewall stopped 100 source routed packets in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

Limiting audit in this manner reduces system load.

Options for viewing the audit output generated by these selections include:

- The Admin Console Dashboard
- **Monitor > Audit**
- Third-party reporting tools

Configure the UDP network defense

The UDP network defense allows you to customize audit output for UDP attacks stopped by the firewall. Follow these steps to configure the **UDP** tab.

Steps

- 1) Select **Policy > Network Defenses > UDP**.
- 2) In the **Audit the selected UDP attacks** section, select the attacks for which you want the firewall to generate audit.



Tip: For option descriptions, click **Help**.

- 3) In the **Audit the selected UDP compliance issues** area, select how you want the firewall to audit packets that are not known attacks, but are still not compliant with the UDP standards. Options are:
 - **Audit all UDP compliance issues**
 - **Audit severe and moderate UDP compliance issues**
 - **Audit severe UDP compliance issues**
 - **Do not audit any UDP compliance issues**

- 4) In the **UDP Audit Frequency** area, select how often to generate audit for UDP issues. Select one of the following:
 - **Limit auditing (recommended)** — Generates an audit record for the first *x* occurrences for every *y* seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed. For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the firewall stopped 100 zero source port UDP attacks in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

Limiting audit in this manner reduces system load.
 - **Always audit** — Generates an audit record for every audit event.



Note: Unlimited auditing runs the risk of overflowing the log partition and creating problems for the firewall.

Options for viewing the audit output generated by these selections include:

- The Admin Console Dashboard
- **Monitor > Audit**
- Third-party reporting tools

Configure the ICMP network defense

The ICMP network defense allows you to customize audit output for ICMP attacks stopped by the firewall. Follow these steps to configure the **ICMP** tab.

Steps

- 1) Select **Policy > Network Defenses > ICMP**
- 2) In the **Audit the selected ICMP attacks** section, select the attacks for which you want the firewall to generate audit.



Tip: For option descriptions, click **Help**.

- 3) In the **Audit the selected ICMP compliance issues** area, select how you want the firewall to audit packets that are not known attacks, but are still not compliant with the ICMP standards. Options are:
 - **Audit all ICMP compliance issues**
 - **Audit severe and moderate ICMP compliance issues**
 - **Audit severe ICMP compliance issues**
 - **Do not audit any ICMP compliance issues**

- 4) In the **ICMP Audit Frequency** area, select how often to generate audit for ICMP issues. Select one of the following:

- **Limit auditing (recommended)** — Generates an audit record for the first x occurrences for every y seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed. For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the firewall stopped 100 invalid redirect ICMP attacks in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

Limiting audit in this manner reduces system load.

- **Always audit** — Generates an audit record for every audit event.



Note: Unlimited auditing runs the risk of overflowing the log partition and creating problems for the firewall.

Options for viewing the audit output generated by these selections include:

- The Admin Console Dashboard
- **Monitor > Audit**
- Third-party reporting tools

Configure the ARP network defense

The ARP network defense allows you to customize audit output for ARP attacks stopped by the firewall. Follow these steps to configure the **ARP** tab.

Steps

- 1) Select **Policy > Network Defenses > ARP**.



Tip: For option descriptions, click **Help**.

- 2) In the **Audit the selected ARP compliance issues** area, select how you want the firewall to audit packets that are not known attacks, but are still not compliant with the ARP standards. Options are:
 - **Audit all ARP compliance issues**
 - **Audit severe and moderate ARP compliance issues**
 - **Audit severe ARP compliance issues**
 - **Do not audit any ARP compliance issues**
- 3) In the **ARP Audit Frequency** area, select how often to generate audit for ARP issues. Select one of the following:
 - **Limit auditing (recommended)** — Generates an audit record for the first *x* occurrences for every *y* seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed. For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the firewall stopped 100 ARP attacks in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

Limiting audit in this manner reduces system load.
 - **Always audit** — Generates an audit record for every audit event.



Note: Unlimited auditing runs the risk of overflowing the log partition and creating problems for the firewall.

Options for viewing the audit output generated by these selections include:

- The Admin Console Dashboard
- **Monitor > Audit**
- Third-party reporting tools

Configure the IPsec network defense

The IPsec network defense allows you to customize audit output for IPsec attacks stopped by the firewall. Unlike the other network defenses, it also allows you to control non-malicious failure audits.

Follow these steps to configure the IPsec tab.

Steps

- 1) Select **Policy > Network Defenses > IPsec**.
- 2) In the **Audit the selected IPsec attacks** section, select the attacks for which you want to generate audit.



Tip: For option descriptions, click **Help**.

- 3) In the **Audit the selected IPsec compliance issues** area, select how you want to audit packets that are not known attacks, but are still not compliant with the IPsec standards. Options are:
 - **Audit all IPsec compliance issues**
 - **Audit severe and moderate IPsec compliance issues**
 - **Audit severe IPsec compliance issues**

- Do not audit any IPsec compliance issues
- 4) In the **IP Audit Frequency** area, select how often to generate audit for IPsec issues. Select one of the following:
- **Limit auditing (recommended)**— Generates an audit record for the first x occurrences for every y seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed. For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the firewall stopped 100 decryption failures in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

Limiting audit in this manner reduces system load.
 - **Always audit** — Generates an audit record for every audit event.



Note: Unlimited auditing runs the risk of overflowing the log partition and creating problems for the firewall.

Options for viewing the audit output generated by these selections include:

- The Admin Console Dashboard
- **Monitor > Audit**
- Third-party reporting tools

Configure the IPv6 network defense

The IPv6 network defense allows you to customize audit output for IPv6 attacks stopped by the firewall.



Note: The **IPv6** tab appears only if IPv6 is enabled on your firewall.

Follow these steps to configure the IPv6 tab.

Steps

- 1) Select **Policy > Network Defenses > IPv6**.
- 2) In the **Audit the selected IPv6 attacks** section, select the attacks for which you want to generate audit.



Tip: For option descriptions, click **Help**.

- 3) In the **Audit the selected IPv6 compliance issues** area, select how you want to audit packets that are not known attacks, but are still not compliant with the IPv6 standards. Options are:
 - **Audit all IPv6 compliance issues**
 - **Audit severe and moderate IPv6 compliance issues**
 - **Audit severe IPv6 compliance issues**
 - **Do not audit any IPv6 compliance issues**
- 4) In the **IP Audit Frequency** area, select how often to generate audit for IPv6 issues. Select one of the following:

- **Limit auditing (recommended)** — Generates an audit record for the first x occurrences for every y seconds. Other occurrences of the same audit event in that window will not be recorded. An additional audit event will be generated to record how many other audit events were suppressed. For example, the audit is limited to generating an audit event for the first three (3) occurrences for every 60 seconds. If the firewall stopped 100 decryption failures in 60 seconds, then it generates three records for the first three denials, and then generates another audit record stating that 97 occurrences were suppressed in that 60 second window.

Limiting audit in this manner reduces system load.

- **Always audit** — Generates an audit record for every audit event.



Note: Unlimited auditing runs the risk of overflowing the log partition and creating problems for the firewall.

Options for viewing the audit output generated by these selections include:

- The Admin Console Dashboard
- **Monitor > Audit**
- Third-party reporting tools

Contents

- [Your SNMP needs](#) on page 345
- [Setting up an SNMP Agent](#) on page 345
- [When to use the SNMP pass-through](#) on page 359

The Simple Network Management Protocol (SNMP) is the industry standard for network management.

Your SNMP needs

Sidewinder supports several SNMP capabilities.

The following protocols are supported:

- SNMP v1
- SNMP v2c
- SNMP v3

SNMP on the firewall might include the following, depending on your needs:

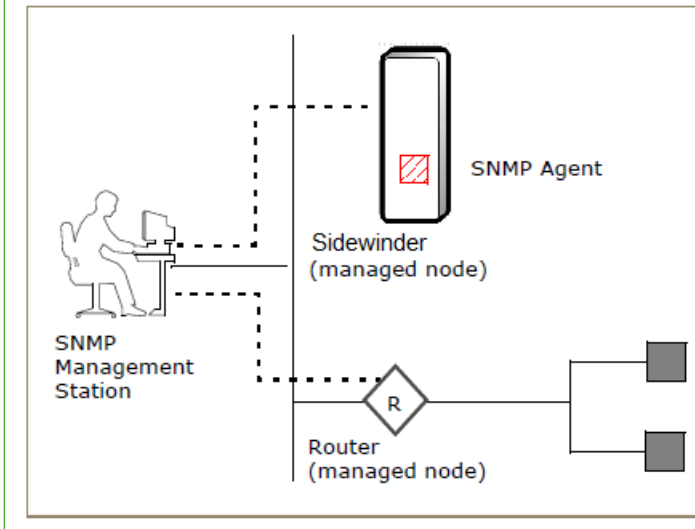
- **SNMP Agent** — Uses the firewall to generate SNMP traps and respond to SNMP queries
- **SNMP pass-through access control rule** (referred to as **SNMP pass-through**) — Sends or routes SNMP messages through the firewall

Setting up an SNMP Agent

You can set up an SNMP Agent software that allows the firewall to operate as an SNMP-managed node.

The node is monitored by SNMP-compliant network management stations located within a firewall zone. Multiple devices report to the management station, and the Sidewinder appliance is one of them.

Figure 45: SNMP management station and firewall SNMP Agent



SNMP management station communication

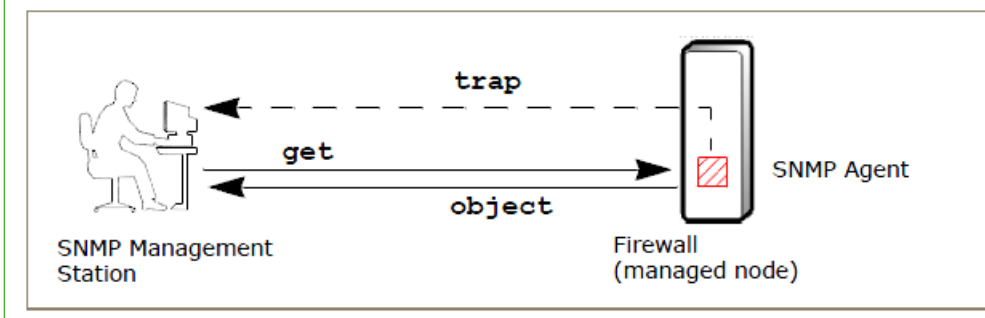
An SNMP-managed network involves two main components.

- **Management station** — Typically a PC or UNIX computer running network management software
- **Number of managed nodes** — Networking devices, such as routers or firewalls, that contain an SNMP Agent

The management station uses management software to display a graphical representation of a network's topology. Network managers monitor SNMP nodes by clicking icons that represent each node in the topology.

The figure shows a management station communicating with an SNMP node to obtain network configuration information.

Figure 46: Communication between a management station and a managed node



A management station in an internal or external network can request information from the SNMP Agent for a managed node:

- The SNMP management station sends get and getnext SNMP messages to a managed node to retrieve objects.
- The managed system responds by providing information such as the node device names, status, and network connections.



Note: SNMP Agents typically allow **Get**, **GetNext**, and **Set requests** from the management station. However, the Sidewinder SNMP Agent does not support **Set requests**. This prevents a management system from sending commands to change firewall variables or parameters.

SNMP traps

When a managed mode detects certain system events, the node can send a *trap*—an unsolicited event notification message—to a management station.

Example: You can configure the firewall audit system to issue a trap whenever an unauthorized user tries to read, write, or execute a protected file on the firewall.

The firewall SNMP Agent supports a basic trap called the *ColdStart trap*. This trap is sent whenever the SNMP Agent is enabled or the Admin Console modifies `/secureos/etc/snmp/snmpd.conf`, the SNMP configuration file.




Note: The ColdStart trap cannot be disabled.

You can configure the firewall to send audit alert SNMP traps when an audit event (such as an attack or system event) triggers a response.

The table lists predefined (default) alert events plus available options for custom traps.

Table 74: Default and custom SNMP traps

Number	Trap
Default traps	
201	<p>NETWORK_TRAFFIC — This trap is sent when the number of traffic audit events written by the various proxies (WWW, Telnet, FTP, etc.) going through the firewall exceeds a specified number in a specified time period. This information can be useful for monitoring the use of the Sidewinder applications by internal users.</p> <p> Note: Network traffic thresholds are reported as number of events per second, and not as number of bytes per second.</p>
202	<p>ATTACK_ATTEMPT — This trap is sent when an attack attempt (that is, any suspicious occurrence) is identified by one of the applications on the firewall. For example, if the Network Services Sentry (NSS) detects a suspicious IP address on an incoming connection, it will issue an attack attempt trap.</p>
203	<p>TE_VIOLATION — This trap is sent when an unauthorized user or process attempts to perform an illegal operation on a file on the firewall.</p>
204	<p>ACCESS_CONTROL — This trap is sent when the number of denied access attempts to applications exceeds a specified number. For example, you could set up your system so that internal users cannot FTP to a certain Internet address. If a user tried to connect to that address, the attempt would be logged as a denial.</p>
205	<p>BAD_PROXY_AUTH — This trap occurs when a user tries to get authenticated to the telnet or FTP proxy and enters invalid data.</p>

Number	Trap
206	PROBE_ATTEMPT — This trap is sent when network probe attempts are detected. A network probe is any time a user attempts to connect or send a message to a TCP or UDP port that either has no application associated with it or it is associated with an unsupported application. To ignore network probe attempts, create an access control rule to the SNMP Agent application probes coming from recognized offenders.
207	FILTER_FAILURE — This trap occurs when the number of e-mail messages or HTTP messages that failed the keyword filter exceed a specified threshold in a specified time period.
208	IPSEC_FAILURE — The trap occurs when the IPSEC subsystem detects a failure in authentication or encryption of network traffic. This can be caused by a number of things ranging from key configuration errors, ISAKMP problems, interoperability issues, and network attacks.
209	FAILOVER_EVENT — This trap is sent any time a Sidewinder changes its status in an HA cluster from secondary to primary, or from primary to secondary.
210	LOG_FILE_OVERFLOW — This trap is sent when the Sidewinder audit logs are close to filling the partition.
211	SYN_FLOOD_ATTACK — This trap is sent when the firewall encounters a SYN attack.
212	UPS_POWER_FAILURE — This trap is sent when a UPS device detects a power failure and the system is running on UPS battery power.
213	UPS_SYSTEM_SHUTDOWN — This trap is sent when a UPS is running out of battery power or has been on battery power for the estimated batter time.
214	LICENSE_EXCEEDED — This trap is sent when users are denied access through the firewall due to a user license cap violation.
226	CRITICAL_COMPONENT_FAILURE — This trap is sent when the firewall detects that a critical component has failed. For example, this trap occurs when daemond detects a software module has failed.
227	VIRUS_MIME_FAILURE — This trap occurs when the number of e-mail or HTTP messages that failed the MIME/Virus/Spyware filter exceeds a specified threshold in a specified time period.
Custom traps	
15	USER_DEFINED_DEFAULT
16	USER_DEFINED_1
17	USER_DEFINED_2
18	USER_DEFINED_3
19	USER_DEFINED_4
20	USER_DEFINED_5
21	USER_DEFINED_6
22	USER_DEFINED_7
23	USER_DEFINED_8
24	USER_DEFINED_9

Number	Trap
25	USER_DEFINED_10

For more information on snmp traps, see the `snmptrap` man page

Related concepts

[Enabling an SNMP trap](#) on page 329

Related tasks

[Ignore network probe attempts](#) on page 328

SNMP MIBs

The management station and managed node contain Management Information Bases (MIBs) that store information about the managed objects.

The SNMP Agent supports a Host MIB (RFC 1514) and two MIB structures:

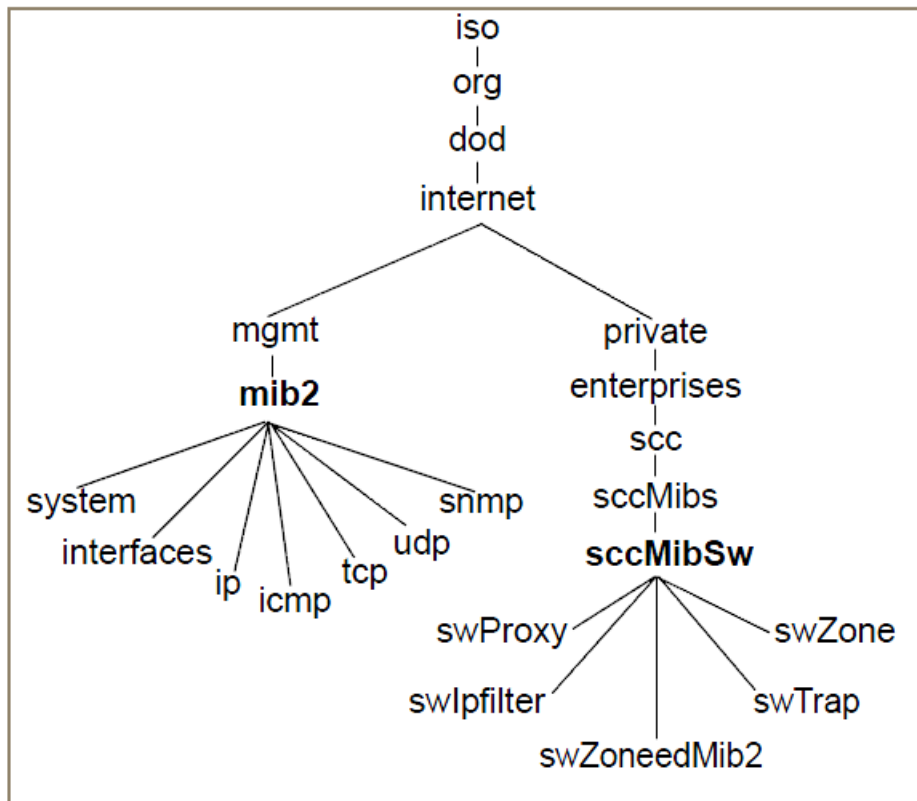
- **mib2** — Standard SNMP MIB (RFC 1213)
- **sccMibSw** — Firewall-specific MIB



Note: MIB files are located in `/secureos/etc/snmp` on the firewall file system.

The figure shows the supported MIB structures and their location in the SNMP root hierarchy.

Figure 47: Firewall MIB structures



The individual objects managed by an SNMP management station are part of an object group within a MIB.

Example: The *swProxy* group stores information about currently defined proxies on the system.



Note: When a management station requests information from the firewall SNMP Agent, the SNMP Agent might or might not associate the response with a specific zone.

Configure the SNMP Agent

This section explains how to configure the SNMP Agent.

Before you begin, consider the following information.

SNMP management station

You will need information to communicate with the firewall and zone.

- Sidewinder host name or IP address for setting up communication with the firewall
- [Conditional] If the zone containing the SNMP Agent has more than one interface, the address for the first interface in the zone

MIB information

You might need this MIB information to properly translate the object identifications.

- The firewall supports the Host Resources MIB.
- The MIB files, SCC-MIB.txt and SCC-SW-MIB.txt, are located on the firewall file system at /secureos/etc/snmp.
- You can access the MIB files on the firewall or download them from the Internet via an FTP client or web browser at <ftp://sidewinder.downloads.forcepoint.com/pub/mibs/>.

Select **Monitor > SNMP Agent**. The **SNMP Agent** window appears.



Tip: For option descriptions, click **Help**.

Use the following procedures to configure the SNMP Agent.

Related tasks

[Add agent information](#) on page 351

[Add, modify, or delete communities](#) on page 351

[Add, modify, or delete SNMP v3 users](#) on page 353

[Select the trap version](#) on page 355

[Add, modify, or delete trap destinations](#) on page 356

[Create a rule](#) on page 357

Add agent information

On the **SNMP Agent** window, add the information described in the table.

Table 75: SNMP Agent fields

Option	Description
Location	[Optional] Type the physical location of the firewall.
Contact	[Optional] Type the user name or email address of the firewall administrator or other contact.
Enable authentication failure trap	Select an option: <ul style="list-style-type: none"> • Yes — Enables SNMP authentication failure traps • No — Disables SNMP authentication failure traps
Allowed Protocols	Select the SNMP versions that incoming SNMP requests are allowed to use.

Add, modify, or delete communities

If you selected **SNMP v1** or **SNMP v2c** in the **Allowed Protocols** area, configure community names to allow the management station to retrieve MIB objects from the SNMP Agent.



Note: The SNMP Agent will not start unless a community name is specified. By default, if you do not specify an Allowed get community name, only Allowed Get Community is “public.”


From the **SNMP Agent** window, use the **Allowed get communities** area to add, edit, or delete communities that are authorized to retrieve MIB information.

The SNMP Agent checks the community name in all incoming v1 and v2c SNMP messages to verify the identity of a manager.



Note: Communities are not used in SNMP v3.

Table 76: SNMP community tasks

Task	Steps
Add a community	<ol style="list-style-type: none"> 1) Click New to add a community. The Allowed Get Community window appears. 2) Type the community name. <div style="margin-left: 20px;">  <p>Tip: The name can contain alphanumeric characters and symbols.</p> </div> 3) Click Add. The community appears in the Allowed get communities pane. 4) Save your changes.
Modify a community	<ol style="list-style-type: none"> 1) Select the community you want to change. 2) Click Modify. The Allowed Get Community window appears. 3) Make your changes, then click OK. 4) Save your changes.
Delete a community	<ol style="list-style-type: none"> 1) Select the community you want to delete. 2) Click Delete. The Confirm Delete message appears. 3) Click Yes to delete or No to cancel the request. 4) Save your changes.

Add, modify, or delete SNMP v3 users





If you selected **SNMP v3** in the **Allowed Protocols** area, you must configure user names and passwords that match the management stations and assign the security level.



Note: All trap destinations use the same SNMP user.

From the **SNMP Agent** window, use the SNMP v3 users pane to add, modify, or delete users who can issue requests to the firewall SNMP Agent.

Table 77: SNMP user tasks

Task	Steps
Add a user	<ol style="list-style-type: none"> <li data-bbox="852 279 1479 342">1) Click New to add a user. The SNMP v3 User window appears. <li data-bbox="852 386 1479 478">2) In the Username field, type the user name that is established on the SNMP management station. <ul style="list-style-type: none"> <li data-bbox="954 499 1471 617">  Tip: The name can contain alphanumeric characters and symbols. <li data-bbox="852 661 1390 724">3) [Optional] In the Description field, add additional information about the user. <li data-bbox="852 768 1422 831">4) In the Password field, type the password established on the management station. <ul style="list-style-type: none"> <li data-bbox="943 852 1471 936">  Note: The password must be at least 8 characters in length. <li data-bbox="852 980 1406 1043">5) In the Confirm Password field, type the password again. <li data-bbox="852 1087 1471 1346">6) In the Minimum security level field, use the drop-down list to select an option for whether authentication and encryption should be used when responding to SNMP messages: <ul style="list-style-type: none"> <li data-bbox="932 1230 1065 1255">• noAuth <li data-bbox="932 1272 1114 1297">• authNoPriv <li data-bbox="932 1314 1078 1339">• authPriv <li data-bbox="852 1390 1390 1556">7) Select the Authentication type. Available options are MD5 and SHA-1. <ul style="list-style-type: none"> <li data-bbox="943 1472 1471 1556">  Note: If FIPS 140-2 processing is enabled, SHA-1 must be selected. <li data-bbox="852 1600 1357 1766">8) Select the Privacy protocol. Available options are DES and AES. <ul style="list-style-type: none"> <li data-bbox="943 1682 1471 1766">  Note: If FIPS 140-2 processing is enabled, AES must be selected. <li data-bbox="852 1810 1471 1873">9) Click Add. The user appears in the SNMP v3 users pane. <li data-bbox="852 1917 1162 1959">10) Save your changes.

Task	Steps
Modify a user	<ol style="list-style-type: none"> 1) Select the user you want to change. 2) Click Modify. The SNMP v3 User window appears. 3) Make your changes, then click OK. 4) Save your changes.
Delete a user	<ol style="list-style-type: none"> 1) Select the user you want to delete. 2) Click Delete. The Confirm Delete message appears. 3) Click Yes to delete or No to cancel the request. 4) Save your changes.

Select the trap version

From the **SNMP Agent** window, select the trap version that the firewall should use when sending traps.

Steps

- 1) In the **Trap version** field, use the drop-down list to select the SNMP version.



Tip: For option descriptions, click **Help**.

- 2) [Conditional] If you selected **v3**, configure the security level to use when sending traps:
 - a) Click **v3 settings**. The **SNMP v3 Trap Settings** window appears.
 - b) In the **Username** field, type the user name established on the SNMP management station.
 - c) In the **Password** field, type the password established on the management station.

Note: The password must be at least 8 characters in length.
 - d) In the **Confirm Password** field, type the password again.
 - e) In the **Security level** field, use the drop-down list to select an option for whether authentication and encryption should be used when responding to SNMP messages:
 - **noAuth**
 - **authNoPriv**
 - **authPriv**

- f) Select the **Authentication type**.
Available options are **MD5** and **SHA-1**.



Note: If FIPS 140-2 processing is enabled, **SHA-1** must be selected.

- g) Select the **Privacy protocol**.
Available options are **DES** and **AES**.



Note: If FIPS 140-2 processing is enabled, **AES** must be selected.



- h) Click **OK**, and save your changes.

Add, modify, or delete trap destinations

Configure the hosts that will receive traps generated by the firewall SNMP Agent.

From the **SNMP Agent** window, use the **Trap destinations** pane to add, modify, or delete a host.

Table 78: SNMP host tasks

Task	Steps
Add a host	<ol style="list-style-type: none"> 1) Click New. The Trap Destination window appears. 2) In the Host name or address field, type the name or IP address of the host. <ul style="list-style-type: none">  Tip: The name can contain alphanumeric characters and symbols. 3) [Optional] In the Community name field, type the community name to associate with this host. <ul style="list-style-type: none">  Note: If you do not specify a community name, the firewall uses the default community name, public. Community names are not used in SNMP v3. 4) Click Add. The host appears in the Trap destinations pane. 5) Save your changes.

Task	Steps
Modify a host	<ol style="list-style-type: none"> 1) Select the host you want to change. 2) Click Modify. The Trap Destination window appears. 3) Make your changes, then click OK. 4) Save your changes.
Delete a host	<ol style="list-style-type: none"> 1) Select the host you want to delete. 2) Click Delete. The Confirm Delete message appears. 3) Click Yes to delete or No to cancel the request. 4) Save your changes.



Tip: Use Attack Responses to manage *when* the firewall sends SNMP traps to the management station.

Related concepts

[Enabling an SNMP trap](#) on page 329

Related tasks

[Create an attack response](#) on page 321

Create a rule

Create an access control rule that allows access from the management station to the firewall SNMP Agent. The management station should reside in a trusted, internal zone.



Note: If you are configuring SNMP on a firewall that is part of an HA cluster, use the HA cluster address for all firewall queries. Specify the shared HA common IP address or host name, not the actual interface address or host name.

Steps

- 1) Create an access control rule with these settings.



Tip: For option descriptions, click **Help**.

- **Application — SNMP Agent**
- **Source Zone** — Select the set of zones (or zone group) that matches the zone or zones of the management station you expect to access the SNMP Agent on the firewall. The SNMP Agent will only accept and respond to management station requests received in one of the configured source zones.
- **Source Endpoint** — [Optional] The management station access control, which consists of the addresses allowed to send SNMP requests to the firewall.
- **Destination Zone** — Must match the source zone or zone group.
- **Destination Endpoint** — [Optional] The firewall address access control, which consists of the addresses on the firewall allowed to receive SNMP requests.



Note: The address family of the source and/destination endpoints must be consistent; for example, IPv4 to IPv4.

The address family of the rule controls the SNMP Agent behavior. If the access control rule specifies only IPv4 endpoints, then the agent will only accept IPv4 requests. It is the same with IPv6 addresses. If both IPv4 and IPv6 endpoints are accepted, the SNMP agent will accept both IPv4 and IPv6 requests.

Host and domain network objects cannot be used as a source or destination endpoint for an SNMP Agent rule.

- 2) Save your changes.

When booting, the firewall issues a ColdStart trap to all configured trap destinations.

Related concepts

[Configuring access control rules](#) on page 197

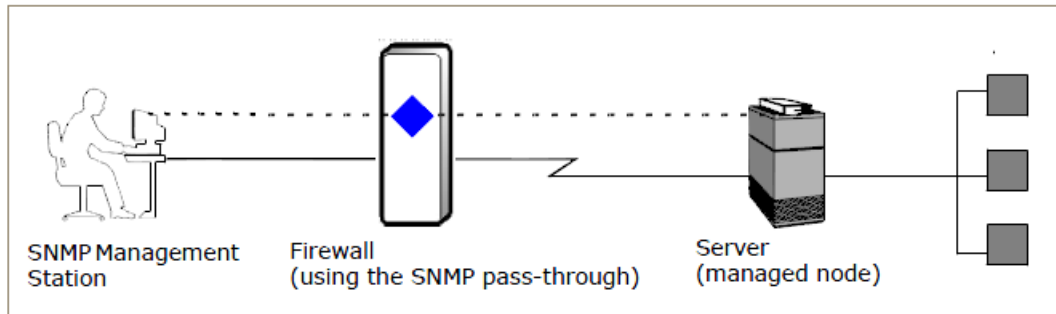
Related reference

[When to use the SNMP pass-through](#) on page 359

When to use the SNMP pass-through

Use the SNMP pass-through when you want to configure the Sidewinder appliance to allow SNMP messages from a management station through the firewall to an SNMP Agent in a different zone.

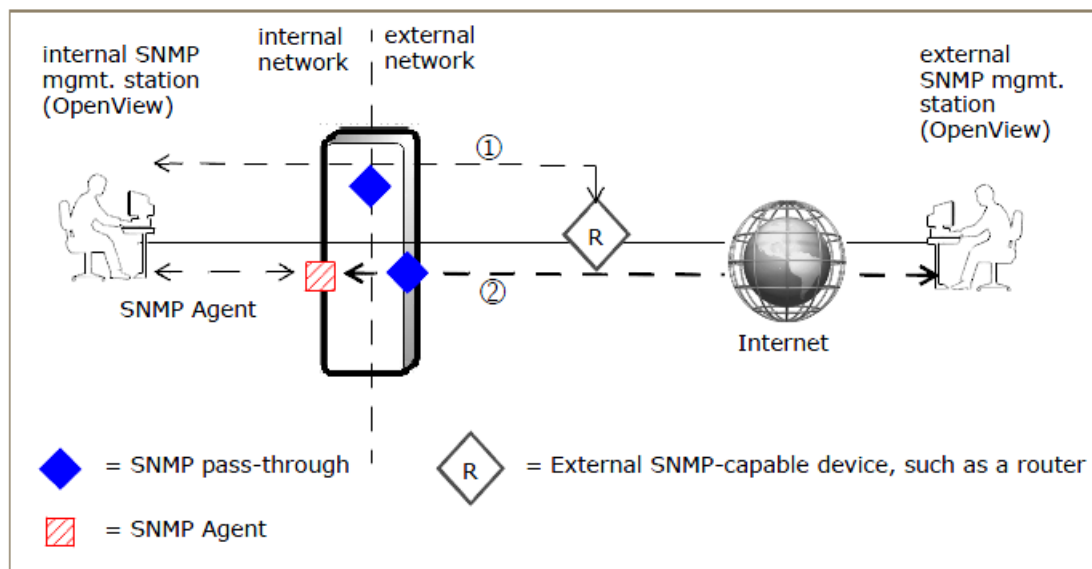
Figure 48: SNMP pass-through



You can route or forward SNMP messages between a management station that is behind the firewall and any SNMP managed node on the other side of the firewall. If your management station is in an untrusted zone or you have multiple management stations in different zones, you can also allow access to the firewall SNMP Agent using the SNMP pass-through in a rule. This section describes scenarios for using the SNMP pass-through and provides guidance on how to set up the access control rules.

The SNMP pass-through routes messages between agents and management stations through the firewall using UDP ports 161 and 162. SNMP traps that originate on the firewall are delivered to the appropriate zones based on the configured trap destinations (no need for the SNMP pass-through).

Figure 49: Firewall as SNMP Agent for internal or external management station



To route SNMP messages, consider this scenario.

From an internal SNMP management station through the firewall via the SNMP pass-through to an external managed node, create an access control rule with the following settings:

- **Action — Allow**

- **Application** — **SNMP**
- **Source Zone** — A single zone that is different from the **Destination Zone**
- **Destination Zone** — A single zone that is different from the **Source Zone**



Tip: The source and destination zones will be different (for example, internal to external).

Related concepts

[Configuring access control rules](#) on page 197

PART IV

Networking

Contents

- [IPv4 and IPv6 overview](#) on page 363
- [Security zones](#) on page 369
- [Interfaces and NICs](#) on page 373
- [Quality of Service](#) on page 397
- [DHCP Relay](#) on page 409
- [Routing](#) on page 413
- [DNS \(domain name system\)](#) on page 459
- [Email](#) on page 487
- [VPN \(virtual private networks\)](#) on page 509

IPv4 and IPv6 overview

Contents

- [Support for IPv4 and IPv6](#) on page 363
- [Firewall IPv4 and IPv6 support by area](#) on page 364
- [Access control rules and IPv6](#) on page 367

Forcepoint Sidewinder supports both IPv4 and IPv6 addresses, allowing you to integrate with more networks.

Support for IPv4 and IPv6

IPv6 support also gives you access to larger blocks of routable addresses.

The following connection types are supported:

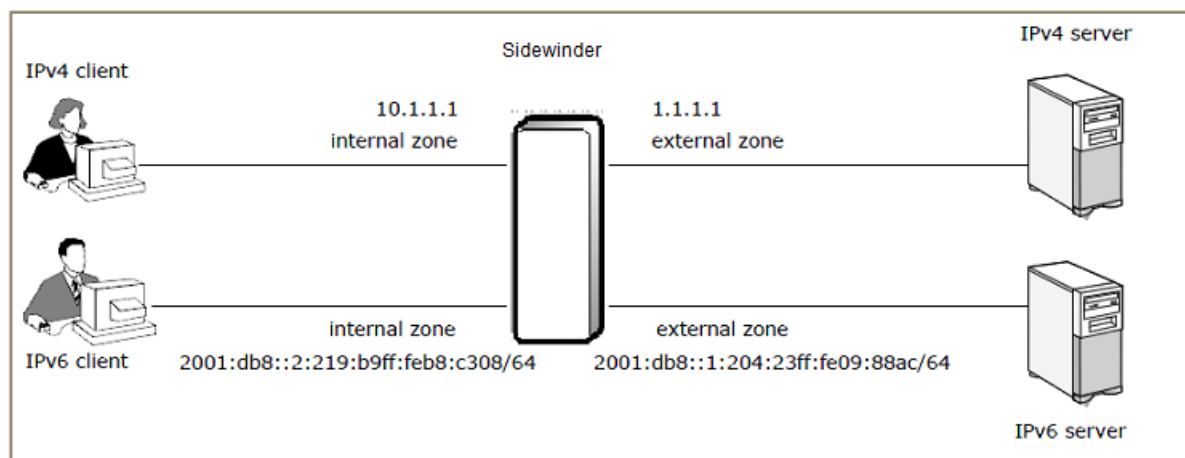
- IPv4-to-IPv4
- IPv6-to-IPv6
- [non-transparent HTTP only] IPv4-to-IPv6



Note: An IPv4 host cannot connect directly to an IPv6 host or vice versa under any circumstances. (For HTTP IPv4-to-IPv6 translation, the firewall is acting as a proxy server, so there is no direct connection between source and destination.)

The firewall can pass both types of traffic using dual stack architecture.

Figure 50: Dual stack architecture



You can also configure Sidewinder to allow IPv4 clients to connect to IPv6 web servers. To successfully connect in this configuration, clients must be configured to use the firewall as a proxy server.

Figure 51: IPv4-to-IPv6 translation








Firewall IPv4 and IPv6 support by area

Some Sidewinder features support IPv4 only, while other features support both IPv4 and IPv6. The table lists IPv4 and IPv6 support by area.

Table 79: IPv4 and IPv6 support by feature

Feature	Supports IPv4	Supports IPv4 and IPv6
Administration methods	<ul style="list-style-type: none"> SF Administration Console Telnet 	<ul style="list-style-type: none"> Admin Console SSH

Feature	Supports IPv4	Supports IPv4 and IPv6
Applications	All applications	<p>Use a generic application on the appropriate port(s) instead of these applications:</p> <ul style="list-style-type: none"> • Telnet • RealMedia • SOCKS • SNMP • Sun RPC • SIP • RTSP • Oracle • SSH • RSH • Citrix-ICA • T120 • SMTP • DNS • H.323 • iiop • MSSQL • Citrix Browser • rlogin <p>All other applications support IPv6</p>
Application Defenses	All Application Defenses	<ul style="list-style-type: none"> • HTTP • Generic <div style="border: 1px solid gray; padding: 5px; background-color: #f0f0f0;"> <p> Note: For all other Application Defenses, settings are ignored for IPv6</p> </div>
Authentication (client connection to firewall)	All authentication methods including Common Access Card (CAC)	All authentication methods including Common Access Card (CAC)
Authentication (firewall connection to authentication server)	All local and remote authentication server types, including Passive Passport (Logon Collector)	<p>Local methods only:</p> <ul style="list-style-type: none"> • Password • Active Passport • Common Access Card (CAC)
Content inspection	<ul style="list-style-type: none"> • Global Threat Intelligence • IPS 	IPS
Static routing	Supported	Supported

Feature	Supports IPv4	Supports IPv4 and IPv6
Dynamic routing	<ul style="list-style-type: none"> BGP RIP PIM-SM OSPF 	<ul style="list-style-type: none"> BGP OSPFv6
High Availability	<ul style="list-style-type: none"> Failover HA Load sharing HA 	Failover HA
HTTP URL translation	Yes	No  Note: If an IPv6 connection matches a URL translation rule, the connection is dropped and an error is audited.
Inter-product communication	Control Center	None  Note: This product can process data that contains IPv6, but not connect using IPv6
Packet filters	All	All
Proxies	<ul style="list-style-type: none"> All proxies 	<ul style="list-style-type: none"> HTTP TCP UDP  Note: FTP will handle IPv6 in the kernel, but not in the proxy. Any number of settings could force an FTP connection to use the proxy, disallowing IPv6.
Servers	<ul style="list-style-type: none"> DHCP Relay sendmail Firewall-hosted DNS (BIND) 	<ul style="list-style-type: none"> Firewall-hosted DNS (BIND) SNMP server
SmartFilter	SmartFilter Admin Console  Note: The SmartFilter Administration Console cannot manage over an IPv6 connection or filter IPv6 traffic	Locally managed SmartFilter

Feature	Supports IPv4	Supports IPv4 and IPv6
VPN (ISAKMP)	<ul style="list-style-type: none"> All VPN modes Client address pools 	Gateway-to-gateway

Access control rules and IPv6

When IPv6 is enabled, two default network objects are available for access control rules and SSL rules to distinguish between endpoints of <Any>.

- <Any V4>
- <Any V6>



Note: At this time, some firewall facilities do not support IPv6. When supported in the future, IPv6 traffic will match those rules.

For access control rules that allow IPv6 traffic, only Application Defenses for the following Application Defense types apply:

- Generic
- HTTP

Application Defenses for other Application Defense types can be included in the Application Defense group contained in the rule, but these additional Application Defenses are ignored for IPv6.

Related concepts

[Allowing IPv6 network flows through the firewall](#) on page 236

Related tasks

[Configure IPv6 addresses](#) on page 390

[Configure IPv4-to-IPv6 translation for HTTP](#) on page 239

Related reference

[Firewall IPv4 and IPv6 support by area](#) on page 364

Security zones

Contents

- [What isolates networks](#) on page 369
- [Configuring zones](#) on page 370

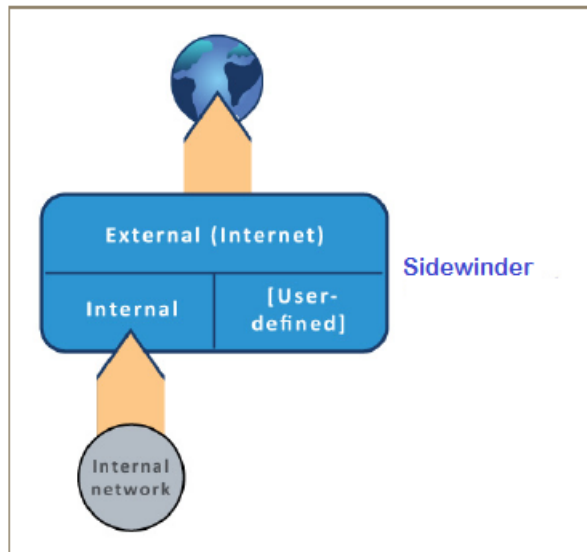
Use zones to assign different policies to your networks.

What isolates networks

Zones are compartments that isolate networks with different security requirements from each other. During the installation process, the Sidewinder appliance automatically sets up two default zones:

- External
- Internal

Figure 52: Security zones



Related concepts

[Configuring zones](#) on page 370

Related information

[Attributes of a network interface](#) on page 373

Configuring zones

When you work with access control rules and SSL rules, you will be asked to select Source and Destination zones. You can create, modify, and delete zones in the **Zone Configuration** window.

Select **Network > Zone Configuration**. The **Zone Configuration** window appears.

- The upper pane lists existing zones and zone groups.
- When you select a zone or zone group in the table, the lower pane displays the properties.



Tip: For option descriptions, click **Help**.

Note the following:

- The firewall supports up to 63 zones.
- At least two zones must exist at all times.
- The current *Internet zone* cannot be deleted. This zone has pre-defined attributes "both configurable and non-configurable" to supply a secure connection to the Internet. You can configure which zone is the Internet zone.
- A *virtual zone* is a zone that does not contain a network interface. Use virtual zones to apply security policy to VPN traffic.



Note: Virtual zones do not support ICMP.

- You can change the default zone names during the initial configuration process.

Related concepts

[Renaming default zones](#) on page 22

Related tasks

[Create or modify a zone](#) on page 370

[Create or modify a zone group](#) on page 371

[Delete a zone or zone group](#) on page 372

Create or modify a zone

The **New Zone** and **Modify Zone** windows are used to create a zone or make changes to an existing zone.

Steps

- 1) [Conditional] To create a new zone, click **New Zone** on the toolbar. The **New Zone** window appears.
- 2) [Conditional] To modify an existing zone, select the zone and click **Modify Zone** on the toolbar. The **Modify Zone** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Zone name** field, type a case-sensitive name for the zone.



Tip: The following naming criteria applies:

- Must contain 1–64 characters
- Must begin with a letter; the name can contain letters, digits, underscores (`_`), and dashes (`-`)



Note: The name cannot be changed on the **Modify Zone** window.

- 4) [Optional] In the **Description** field, type a more detailed description of the zone.
- 5) In the **Connection Options** area, select one or more of the following options to apply to this zone.
- **Application discovery** — The firewall audits the data for each application that originates in that zone.
 - **Honor ICMP redirect** — The firewall honors ICMP redirects.
 - **Respond to ICMP echo and timestamp** — The firewall responds to these messages.
 - **Hide port unreachables** — If a node on the network attempts to connect to a port that the firewall is not listening on, the firewall ignores the request.



Note: Do not select this option for a heartbeat zone in an HA cluster.

- 6) [Optional] In the **Groups** list, select one or more zone groups to associate the zone with.
- 7) Click **OK**, and save your changes.

Create or modify a zone group

Zone groups provide the means for applying a access control rules and SSL rules to multiple zones. When you select a zone group in the **Source** and **Destination** areas for a rule, you apply that rule to each zone in the zone group.

Use the **New Zone Group** and **Modify Zone Group** windows to create a zone group or make changes to an existing zone group.

Steps

- 1) [Conditional] To create a new zone group, click **New Zone Group** on the toolbar. The **New Zone Group** window appears.
- 2) [Conditional] To modify an existing zone, select the zone and click **Modify Zone Group** on the toolbar. The **Modify Zone Group** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Group name** field, type a name for the zone group. The name cannot be changed on the **Modify Zone Group** window.
- 4) [Optional] In the **Description** field, type a more detailed description of the zone group.

- 5) In the **Zones** list, select one or more zones to associate with this group.
- 6) Click **OK**, and save your changes.

Delete a zone or zone group

You can delete a zone or zone group from the **Zone Configuration** window.

Steps

- 1) Determine whether the zone or zone group is currently being used.



Tip: For option descriptions, click **Help**.

- a) Select the zone or zone group you want to delete.
- b) Click **Usage**.
 - If the zone or zone group is currently being used, the **Usage** window appears listing every area where the zone or zone group is currently used. Before you can delete the zone or zone group, you must remove it from use.
 - If the zone or zone group is not currently being used, a message appears confirming that.
- 2) With the zone or zone group highlighted, click **Delete**. The **Confirm Delete** dialog appears.
 - To delete the zone or zone group, click **Yes**.
 - To cancel the action, click **No**.

Interfaces and NICs

Contents

- [Attributes of a network interface](#) on page 373
- [Manage interfaces](#) on page 380
- [Manage NICs and NIC groups](#) on page 392
- [Test connectivity for an interface or NIC](#) on page 395

A Sidewinder interface is a logical representation of a network connection.

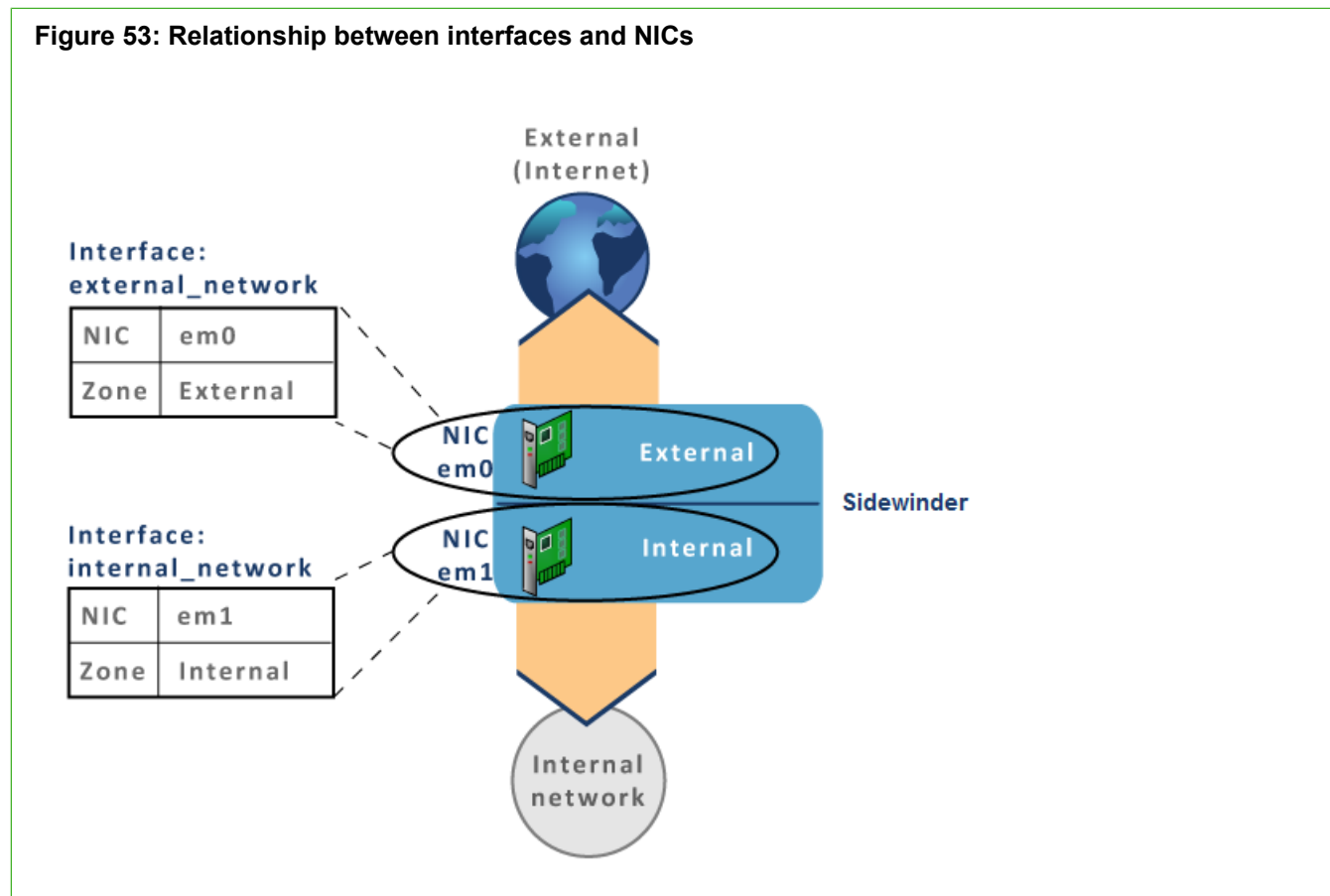
This representation includes the following attributes:

- NIC or NIC group
- VLAN ID
- MTU size (maximum transmission unit)
- Zone
- IP addresses
- Quality of Service profile

Attributes of a network interface

The network interface card (NIC) or NIC group serves as the hardware device that connects the firewall to a network.

The relationship between interfaces and NICs allows you to easily move your network configuration to different network hardware by assigning a different NIC to the interface.

Figure 53: Relationship between interfaces and NICs

Types of interfaces

You can create and configure the following types of interfaces and interface elements.

- Standard interfaces
- VLAN interfaces
- DHCP interfaces
- Transparent interfaces
- SPAN interfaces
- High Availability interfaces

Standard interfaces

A standard interface is a single interface with a static IP address assigned.

Related tasks

[Create a standard interface](#) on page 381

VLAN interfaces

A VLAN interface is a virtual interface that segments a LAN into different broadcast domains regardless of the physical location. By using VLANs, you can create up to 512 interfaces on a standalone firewall and 255 interfaces on a High Availability (HA) cluster.

Considerations for VLAN interfaces:

- VLANs might not work on some older NICs.
- You must use a network switch or router that can decipher VLAN traffic.
- VLANs are supported in an HA configuration. For best results, configure VLANs before configuring HA.
- To filter traffic for a VLAN, use the following syntax:
 - **NIC** — `tcpdump -pni nic vlan vlanID`
 - **NIC group** — `tcpdump -pni nic_group vlan vlanID`

Related tasks

[Create a VLAN interface](#) on page 383

DHCP interfaces

A DHCP interface is an interface that allows you to centrally manage IP addresses with your network using the Dynamic Host Configuration Protocol.

Considerations for DHCP interfaces:

- Only one DHCP interface can be enabled at a time.
- DHCP interfaces are not allowed on an HA cluster.

Related tasks

[Create a DHCP interface](#) on page 382

Transparent interfaces

A transparent interface is made up of two or more bridged interfaces. Use a transparent interface to separate a single Ethernet segment into two or more zones. This allows you to enforce security policy on traffic that passes through the transparent interface without re-addressing the network around the firewall.

- The firewall supports only one configured transparent interface (bridge) at a time.
- Each bridged interface must be associated with a unique zone.

This table shows the default Sidewinder interface configuration. These interfaces or any other interfaces can be used to configure a transparent interface.

Table 80: Standard interfaces

User-defined interface name	NIC or NIC group	Zone name
external_network	em0	external
internal_network	em1	internal

This table shows a configured transparent interface using the default interfaces. Notice that bridge0 is made up of em0 and em1.

Table 81: Transparent interface

User-defined transparent interface name	NIC or NIC group
bridged_network	bridge0 (em0, em1)

When you configure a transparent interface, you cannot enable or configure:

- Split DNS
- HA
- Sendmail
- Dynamic routing
- DHCP on the transparent interface
- DHCP Relay agent
- VPN termination in a transparent zone
- IPv6 addresses on the transparent interface



Note: A transparent interface passes traffic at layer two, similar to a bridge. Sidewinder does not run the Spanning Tree bridging protocol; therefore, we do not recommend enabling Spanning Tree on the switch that is connected to the firewall.

Related tasks

[Create a transparent interface](#) on page 384

SPAN interfaces

A SPAN interface allows the firewall to monitor network traffic without placing the firewall directly in the network path.

In SPAN mode, the firewall interface is connected to a SPAN port on the switch. The firewall receives copies of all network packets the switch handles, called *port forwarding* or *port mirroring*.



Note: If the firewall is part of a High Availability cluster, SPAN interfaces cannot be configured.

If SPAN mode is enabled on an interface, the following configurations are not supported for that interface or zone:

- NIC groups
- Transparent or bridged interface
- MTU size
- DHCP
- IPv4 or IPv6 addresses
- Quality of Service profiles
- Internet zone
- All firewall-hosted servers (such as Admin Console, sendmail, dynamic routing)

Related tasks[Create a SPAN interface](#) on page 385[Create a SPAN policy](#) on page 272

High Availability interfaces

If a firewall is part of an HA cluster, the **Interface Properties** window has two IP addresses.

- **Cluster IP address** — This is the IP address for the interface in the HA cluster.
- **Primary IP address** — This is the IP address of the interface before joining the HA cluster.



Note: You cannot use IPv6 addresses in a Load Sharing HA cluster. However, Failover HA clusters support IPv6.

If you modify any of these attributes in an interface, the same modification is automatically made in the corresponding interface for the other cluster member:

- Zone
- Quality of Service profile
- Alias address
- MTU



Note: If you make configuration changes to an HA cluster interface, both cluster firewalls must be restarted.

Related tasks[Create a High Availability interface](#) on page 386[Restart an HA cluster](#) on page 658

Interfaces and IP addresses

The external and internal network interfaces are defined during initial configuration, and these interfaces have IPv4 addresses. An interface can have IPv4, IPv6, or both types of addresses.

IPv4 and IPv6 addresses

IPv4 and IPv6 addressing is available for specific types of interfaces as shown in the following table.



Note: An interface with SPAN enabled cannot be assigned IP addresses.

Table 82: IPv4 and IPv6 addressing for specific interfaces

Interface type	IPv4	IPv6
Standard	X	X

Interface type	IPv4	IPv6
Transparent	X	
HA (Failover)	X	X
HA (Load Sharing)	X	

Related tasks

[Configure IPv4 addresses](#) on page 388

[Configure IPv6 addresses](#) on page 390

Alias IP addresses

Alias IP addresses are used in Multiple Address Translation (MAT).

If you use address masquerading, specific logical networks that are connected to one interface can be consistently mapped to specific IP aliases on another interface.

The interface can:

- Accept connection requests for any defined alias
- Communicate with more than one logical network without a router
- Contain more than one address on the same network and have DNS resolve different domains to each host address

Rules between NICs and interfaces

When creating an interface, you select an available NIC or NIC group. NICs and NIC groups are configured separately from the interface.

Sidewinder uses the following interface–NIC association rules:

- A NIC can be referenced by only one enabled non-VLAN interface.
- A NIC can be referenced by multiple enabled VLAN interfaces.
- A NIC cannot be referenced by enabled VLAN and non-VLAN interfaces simultaneously.



Note: These rules do not apply to disabled interfaces. For example, multiple interfaces can reference the same NIC as long as only one of those interfaces is enabled at a time.

NIC groups

Link Aggregation Groups (LAG) allow you to bundle multiple NICs into a group. Sidewinder offers two types of NIC groups' aggregate for increased bandwidth and redundant for backup purposes.

Considerations for NIC groups:

- All NICs in a group must have the same media capabilities enabled.
- A NIC can be a member of multiple NIC groups, but it can be referenced by only one enabled interface at a time.
- A NIC group allows up to 32 NICs. We recommend the following:
 - **Aggregate** — Three NICs per Aggregate group; your results might vary based on your specific hardware

- **Redundant** — Up to four NICs per Redundant group



Note: The NIC group feature—both aggregate and redundant—is not supported on virtualized computers. A virtual machine host can perform this functionality. For options, refer to your virtual machine host documentation.

You can use aggregate and redundant groups on a standard, VLAN, DHCP, or transparent interface.



Note: NIC groups are not supported on SPAN interfaces.

Related tasks

[Create a NIC group](#) on page 393

Aggregate groups

Aggregate groups use the Link Aggregation Control Protocol (LACP) and the Marker protocols defined by IEEE 802.1AX (formerly known as IEEE 802.3ad).

LACP negotiates a set of aggregate links with the peer. The peer can be a switch that supports LACP or another system that supports LACP when directly connected to the firewall using crossover cables.

An Aggregate group is composed of a primary NIC and peer NICs. All peer NICs in this group inherit the MAC address and MTU of the primary NIC. The primary NIC and all peer NICs in this group share the job of passing traffic to the connected switch. The goal is to create a virtual NIC that provides you with increased bandwidth.

In an Aggregate group, the available bandwidth does not increase for a single conversation. All packets associated with a conversation are transmitted on the same link to maintain the packet order. Aggregate mode achieves a high bandwidth only when there are multiple, simultaneous conversations.



Note: Before you enable an Aggregate group on the firewall, make sure your connected switches are properly configured and segmented. Switches with dynamic LACP enabled might place all LACP traffic in the default VLAN. This can create a traffic loop in your network. To avoid this problem, configure your switch for static LACP (Aggregate) groups that are assigned to different segmented VLANs.

LACP combines bandwidths using only the NICs in the group that share the highest bandwidth and requires all active NICs in the Aggregate group to be full duplex.

Example: If you create an Aggregate group with the following four active NICs, the Aggregate group will have a bandwidth of 2 gigabits.

- **NIC 1** — 1 gigabit
- **NIC 2** — 1 gigabit
- **NIC 3** — 100 megabits
- **NIC 4** — 100 megabits

You can add NICs of different speeds and duplex; however, only the NICs operating at the highest speed and at full duplex are selected to pass traffic.

As the firewall determines which NIC to use, it considers the following variables:

- Source and destination MAC addresses
- Source and destination IPv4/IPv6 addresses
- IPv6 flow label
- VLAN tag

- Number of NICs in the group
- Bandwidth and duplex of each NIC

If you anticipate many different users and sessions connecting to many different destinations on an interface, an Aggregate group is a good choice.

Redundant groups

A *Redundant* group is composed of a primary NIC and standby NICs. The goal here is increased availability.

The primary NIC passes all traffic. If the primary NIC fails (for example, disconnects), the next standby NIC takes over, passing traffic until the primary NIC is restored. When the link for the primary NIC is active again, a failback event automatically occurs, and the primary NIC passes traffic. More than one standby NIC is permitted.



Note: There might be a delay before the standby NIC starts passing traffic while the switch or router recognizes the change and selects the appropriate port.

The NIC group uses the MAC address of the primary NIC for communication at the data-link layer, regardless of which NIC is actively passing traffic. Sidewinder verifies a link at the physical layer (layer 1) and inspects the carrier detect status on the primary NIC in the NIC group.

- If the link is active, the primary NIC passes traffic.
- If the link is inactive, a failover event occurs, and the standby NIC starts passing traffic.



Note: The firewall does not verify communication at the network layer with the next device. A failure in this part of the connection does not trigger a failover event.

Manage interfaces

Create and maintain interfaces from the **Interface Configuration** tab.

Steps

- 1) Select **Network > Interfaces**. The **Interface Configuration** tab appears.



Tip: For option descriptions, click **Help**.

- 2) Use the **Interface Configuration** tab to perform these tasks:

Create an interface

You can create and configure the following types of interfaces and interface elements.

Create a standard interface

Create and configure a standard interface.

Steps

- 1) Click **New** > **Standard Interface**. The **Interface Properties** window appears.



Tip: For option descriptions, click **Help**.

- 2) Enter a name and description for the interface.



Tip: The name can contain:

- Alphanumeric characters
- Dashes (-)
- Underscores (_)
- Spaces ()

- 3) From the **NIC or NIC Group** drop-down list, select the NIC or NIC group to associate with this interface.



Tip: To make changes to the NIC or NIC group hardware properties, click **Modify NIC or NIC group**.

- 4) Select the MTU size for *outgoing* packets.
- 5) From the **Zone** drop-down list, select the zone the interface is in, or click **New zone** to create a zone.
- 6) Enter the IPv4 addresses and aliases to associate with this interface.
- 7) [Optional] Enter the appropriate IPv6 addresses.



Note: You must enable IPv6 on this interface in order to enter IPv6 addresses.

- 8) [Optional] From the **Quality of Service Profile** drop-down list, select a profile for allocating available bandwidth to traffic that is leaving this interface.
- 9) Click **OK**, and save your changes.

Related concepts

[Standard interfaces](#) on page 374

Related tasks[Configure IPv4 addresses](#) on page 388[Configure IPv6 addresses](#) on page 390

Create a DHCP interface

Create and configure an interface that will have its address assigned using DHCP.

Steps

1) Select **Network > Interfaces**. The **Interface Configuration** tab appears.

2) Click **New > Standard Interface**. The **Interface Properties** window appears.



Tip: For option descriptions, click **Help**.

3) Enter a name and description for the interface.



Tip: The name can contain:

- Alphanumeric characters
- Dashes (-)
- Underscores (_)
- Spaces ()

4) From the **NIC** or **NIC Group** drop-down list, select the NIC or NIC group to associate with this interface.



Tip: To make changes to the NIC or NIC group hardware properties, click **Modify NIC** or **NIC group**.

5) Select the MTU size for *outgoing* packets.

6) From the **Zone** drop-down list, select the zone the interface is in, or click **New zone** to create a zone.

7) In the **Address Configuration** area, select **Obtain an IPv4 address automatically via DHCP**.



Note: The internet zone is automatically selected in the **Zone** field and cannot be modified. The **IPv4 addresses** area is disabled; you cannot add an IPv4 address or aliases.

8) [Optional] From the **Quality of Service Profile** drop-down list, select a profile for allocating available bandwidth to traffic that is leaving this interface.

9) Click **OK**, and save your changes.

Related concepts[DHCP interfaces](#) on page 375

Create a VLAN interface

Use this task to create and configure a VLAN interface.

Steps

- 1) Click **New** > **Standard Interface**. The **Interface Properties** window appears.



Tip: For option descriptions, click **Help**.

- 2) Enter a name and description for the interface.



Tip: The name can contain:

- Alphanumeric characters
- Dashes (-)
- Underscores (_)
- Spaces ()

- 3) From the **NIC or NIC Group** drop-down list, select the NIC or NIC group to associate with this interface.



Tip: To make changes to the NIC or NIC group hardware properties, click **Modify NIC or NIC group**.

- 4) Select **VLAN id**.

- 5) In the VLAN id field, specify a numeric ID for this VLAN.

- Valid values are 2–4094 (1 is reserved for special configurations).
- VLAN IDs must be unique across all VLAN interfaces tied to the same physical NIC or NIC group.

- 6) Select the MTU size for *outgoing* packets.

- 7) From the **Zone** drop-down list, select the zone the interface is in, or click **New zone** to create a zone.

- 8) Enter the IPv4 addresses and aliases to associate with this interface.

- 9) [Optional] Enter the appropriate IPv6 addresses.



Note: You must enable IPv6 on this interface in order to enter IPv6 addresses.

- 10) [Optional] From the **Quality of Service Profile** drop-down list, select a profile for allocating available bandwidth to traffic that is leaving this interface.

- 11) Click **OK**, and save your changes.

Related concepts

[VLAN interfaces](#) on page 375

Related tasks[Configure IPv4 addresses](#) on page 388[Configure IPv6 addresses](#) on page 390

Create a transparent interface

Create a transparent interface and assign interface members for the bridge.



Note: The firewall supports only one configured transparent interface (bridge) at a time.

Steps

- 1) Click **New > Transparent Interface**. The **Interface Properties (Transparent)** window appears.



Tip: For option descriptions, click **Help**.

- 2) Enter a name and description for the interface.



Tip: The name can contain:

- Alphanumeric characters
- Dashes (-)
- Underscores (_)
- Spaces ()

- 3) In the **Bridged Interfaces** area, select the checkboxes for the interfaces that will be members of this transparent interface.

Considerations for selecting interfaces:

- You must select two or more member interfaces.
 - Each member interface must be associated with a unique zone.
 - The members can be standard, VLAN, or redundant interfaces.
 - If the members have IP addresses assigned to them, these addresses will be removed when the transparent interface is created.
 - Before being added to a transparent interface, the members must be:
 - Assigned a name
 - Associated with a NIC or NIC group
 - Assigned to a unique zone
- 4) If any of the interfaces you want to bridge are not yet configured, configure them now. From the **Bridged Interfaces** toolbar, click **New**.
 - 5) Select the MTU size for *outgoing* packets.
 - 6) In the **IPv4 addresses** area, enter the appropriate IP addresses and aliases to associate with this interface.



Note: You cannot use IPv6 addresses in a transparent interface.

- 7) Click **OK**, and save your changes.

Related concepts

[Deployment options](#) on page 23

[Transparent \(bridged\) mode deployment](#) on page 25

Create a SPAN interface

Create and configure a SPAN interface.

Steps

- 1) From the Admin Console, select **Network > Interfaces**.
- 2) Select **New > Standard Interface**. The **Interface Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Enter a name and description for the interface.



Tip: The name can contain:

- Alphanumeric characters
- Dashes (-)
- Underscores (_)
- Spaces ()

- 4) Select **Enable SPAN**.
- 5) From the **NIC or NIC Group** drop-down list, select the NIC to associate with this interface. A SPAN interface must be assigned to a single NIC.



Note: NIC groups are not supported for SPAN interfaces.



Tip: To make changes to the NIC configuration, click **Modify NIC or NIC group**.

- 6) If the SPAN interface will process VLAN traffic, configure VLAN properties.
 - a) Select **VLAN id**
 - b) In the **VLAN id** field, specify a numeric ID for this VLAN.
 - Valid values are 2–4094 (1 is reserved for special configurations).
 - VLAN IDs must be unique across all VLAN interfaces tied to the same physical NIC.
- 7) From the **Zone** drop-down list, select the zone the interface is in, or click **New zone** to create a zone.



Note: Select a zone that is not referenced by any non-SPAN interfaces.

- 8) Click **OK**, and save your changes.

Result



Note: If you are using Forcepoint Sidewinder, Virtual Appliance, you will need to enable Promiscuous Mode on the virtual switch used in the SPAN configuration.

Related concepts

[SPAN interfaces](#) on page 376

Create a High Availability interface

Create and configure a High Availability interface. You must create the HA interface on each member of the High Availability cluster.

Steps

- 1) Create the HA interface on a cluster member.
 - a) Select **Network > Interfaces**, then select one of the cluster members listed. The **Interface Configuration** tab appears.
 - b) Click **New**. The **Interface Properties** window appears.



Note: Two addresses are shown: a cluster address and a primary address.



Tip: For option descriptions, click **Help**.

- c) Complete the fields for the interface. Be sure to enter the IP address for the cluster in the **cluster Address/Mask** field.
 - d) Click **OK**, and save your changes.
- 2) Re-create the cluster interface on the other cluster member.
 - The following fields must be identical:
 - **Zone**
 - **Address/Mask (cluster)**



Tip: Use the same NIC or NIC group for each member of the HA cluster that runs on the same hardware.

- Member addresses must be in the same subnet.

Related concepts

[High Availability interfaces](#) on page 377

[Configuring HA](#) on page 644

Modify an interface

You can change the attributes of an interface that is already configured.

Steps

- 1) Select the interface that you want to modify.
- 2) Click **Modify**. The **Interface Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Modify the interface as necessary, then click **OK**.
- 4) Save your changes.

Swap interface parameters

Swapping interface parameters essentially swaps the names of the selected interfaces. The NIC is still associated with the same IP address, zones, and other attributes.

Steps

- 1) Select the first interface.



Tip: For option descriptions, click **Help**.

- 2) Press and hold **Ctrl**, then select the second interface.
- 3) Click **Swap Parameters**. The interface names are exchanged.
- 4) Save your changes.

Delete an interface

When you delete an interface, its attributes are removed and the associated NIC or NIC group is disabled.

Steps

- 1) Select the interface that you want to delete.



Tip: For option descriptions, click **Help**.

- 2) Click **Delete**. A confirmation pop-up appears.
- 3) Click **Yes**.

- 4) Save your changes.

Rename an interface

Rename an interface when you want to change its display name.

Steps

- 1) Select the interface that you want to rename.



Tip: For option descriptions, click **Help**.

- 2) Click **Rename**. The **Rename** window appears.
- 3) Type a name in the **New name** field.
- 4) Click **OK**.
- 5) Save your changes.

View interface status

View the status of an interface.

Click **Show Status**. The **Interface and NIC Status** window appears.



Tip: For option descriptions, click **Help**.

Manage interface IP addresses

Create and maintain IPv4 and IPv6 addresses for existing interfaces.

Configure IPv4 addresses

Configure IPv4 addresses for an existing interface.

Steps

- 1) Select **Network > Interfaces**. The **Interfaces** tab appears.

- 2) Select the interface that you want to manage IP addresses for, then click **Modify**. The **Interface Properties** window appears.

In the **IPv4 addresses** area, the first IP address is the primary address for the interface. All subsequent addresses are aliases.



Tip: For option descriptions, click **Help**.

- 3) Use the IPv4 addresses area to perform the following tasks:

Define a primary IPv4 address

Use this task to define an IPv4 address to associate with the interface.

Steps

- 1) Click the **x.x.x.x/24** field, and type an IPv4 address to associate with this interface.



Tip: For option descriptions, click **Help**.

- 2) [Optional] Modify the network mask, which is used to identify the significant portion of the IP address. Valid values are 0–32.
- 3) Press **Enter**.

Create alias IPv4 addresses

Use this task to create an alias IP address.

Steps

- 1) In the IPv4 addresses area, click **New**.



Tip: For option descriptions, click **Help**.

- 2) Click the **x.x.x.x/24** field, and type an alias IP address to associate with this interface IP address.
- 3) [Optional] Modify the network mask, which is used to identify the significant portion of the IP address. Valid values are 0-32.
- 4) Press **Enter**.

Re-order IPv4 addresses

In the IPv4 addresses area, the first address in the list is the primary address and, when sending data, the outgoing address. You can swap the primary and alias addresses, and you can change the order of the aliases.

Use this task to change the order of the addresses.

Steps

- 1) Select an address.



Tip: For option descriptions, click **Help**.

- 2) Click the **Move up** or **Move down** arrow.

Delete an IPv4 address

Delete an IPv4 address from an interface.

Steps

- 1) In the **IPv4 addresses** area, select the address you want to delete.



Tip: For option descriptions, click **Help**.

- 2) Click **Delete**.

Configure IPv6 addresses

Configure IPv6 addresses for an existing interface.

Steps

- 1) Select **Network > Interfaces**. The **Interfaces** tab appears.
- 2) Select the interface that you want to manage IP addresses for, then click **Modify**. The **Interface Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Use the **IPv6 addresses** area to perform the following tasks:

Create an IPv6 address

Use this task to enable IPv6 and enter addresses.

Steps

- 1) In the **IPv6 addresses** area, select the **Enable IPv6 on this interface** checkbox.



Tip: For option descriptions, click **Help**.

2) Select a stateless auto-address configuration.



Note: Host and router modes should only be used if you want to use autoconfiguration. These modes can cause unexpected results. For example, when an interface is configured in host mode, a firewall can automatically add new IPv6 addresses to the interface that the user might not expect. When an interface is configured in router mode with static IPv6 addresses, if the `rtadvd.conf` file is not modified, the firewall can advertise prefixes derived from the static IPv6 addresses. This can result in unexpected addresses being added to IPv6 devices in the same network operating in host mode.

- **Static** — This mode is the most suitable configuration for most firewalls. The interface is assigned the link-local address plus any static addresses you enter. The link-local address is automatically created whenever an interface becomes enabled.
- **Host mode** — The interface is assigned the link-local address plus any static addresses you enter. It is also assigned autoconfigured addresses derived by combining any prefixes received in router advertisements with the interface ID.
- **Router mode** — The interface is assigned the link-local address plus any static addresses you enter. The firewall sends out router advertisements either with prefixes in the `rtadvd.conf` file or with prefixes derived from the static addresses on the interface.

3) Enter an IPv6 address.

- a) In the IPv6 addresses area, click **New**.
- b) Click the **xxxx** field, and type an IPv6 address to associate with this interface.
- c) [Optional] Modify the mask length, which is used to identify the significant portion of the IP address. Valid values are 0–128.
- d) Press **Enter**.

4) [Optional] Modify the interface ID.

The 16-hexadecimal interface ID is automatically created. By default, it is derived from the NIC or NIC group MAC address and used to generate the link-local address for the interface.

Result



Note: Create a default route that forwards IPv6 traffic with no known route to its destination address.

Related concepts

[Configuring static routes](#) on page 414

Re-order IPv6 addresses

The order of the IPv6 addresses is one of several factors that determine which address is used when the firewall initiates an IPv6 connection. In general, the first address that has the correct scope for a given situation is used.

Use this task to change the order of the addresses.

Steps

- 1) Select an address.



Tip: For option descriptions, click **Help**.

- 2) Click the **Move up** or **Move down** arrow.

Delete an IPv6 address

Delete an IPv6 address from an interface.

Steps

- 1) In the **Address/Mask** list, select the address you want to delete.



Tip: For option descriptions, click **Help**.

- 2) Click **Delete**.

Manage NICs and NIC groups

Create and maintain NICs and NIC groups from the **NIC and NIC Group Configuration** tab.



Note: The firewall automatically detects NICs. To delete an individual NIC, you must physically remove it.

Steps

- 1) Select **Network > Interfaces > NIC and NIC Group Configuration**. The **NIC and NIC Group Configuration** tab appears.



Tip: For option descriptions, click **Help**.

- 2) Use the **NIC and NIC Group Configuration** tab to perform these tasks:

Create a NIC group

Create an aggregate or redundant NIC group.

Steps

- 1) From the **NIC and NIC Group Configuration** tab or the **NIC or NIC Group** area of the **Interface Properties** window, click **Create new NIC group**, then select one of the following:

- **New Aggregate group**
- **New Redundant group**



Note: The group name is automatically assigned and cannot be changed.

The **NIC Group Properties** window appears.



Tip: For option descriptions, click **Help**.

- 2) [Optional] In the **Description** field, add additional information to identify the NIC group. This description appears on the **NIC and NIC Group Configuration** tab.
- 3) Select NICs for the NIC group:
 - a) In the **Available NICs** pane on the left, select the NIC (use the **Ctrl** key to select multiple NICs).
 - b) Click the right arrow to move the selections to the **Selected NICs** pane on the right. The NICs in this pane are members of the NIC group.
- 4) To change the order of a NIC, select it, then use the up and down arrows. The first NIC in the list is the primary NIC.
- 5) Click **OK**.

Delete a NIC group

Delete a NIC group.



Note: You cannot delete a NIC group that is referenced by an interface.

Steps

- 1) **SelectNetwork > Interfaces > NIC and NIC Group Configuration**. The **NIC and NIC Group Configuration** tab appears.



Tip: For option descriptions, click **Help**.

- 2) Select the NIC group.
- 3) Click **Delete**. A message appears asking you to confirm the deletion.

- 4) Click **Yes**.

Modify NIC hardware properties

Modify the media capabilities and media type of a NIC.

Steps

- 1) Select **Network > Interfaces > NIC and NIC Group Configuration**. The **NIC and NIC Group Configuration** tab appears.



Tip: For option descriptions, click **Help**.

- 2) Select the NIC.
- 3) Click **Modify**. The **NIC and NIC Group Configuration: Network Interface Card Properties** window appears.
- 4) Select media type and capabilities.
- 5) Click **OK**.

Restart a NIC

Restart the NIC for a down interface.

Steps

- 1) Select **Network > Interfaces**. The **Interfaces** window appears.
- 2) On the **Interface Configuration** tab or the **NIC and NIC Group Configuration** tab, click **Show Status**. The **Interface and NIC Status** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the table, select the down interface. (The **Up** column checkbox clears.)
- 4) Click **Restart NIC**.

Swap NIC and NIC group parameters

Switch the configuration settings between two NICs, two NIC groups, or a NIC and a NIC group.

Swapping parameters changes the IP address, zones, aliases, and other configured attributes associated with the NIC or NIC group, and different rules are applied. If you swap a NIC and a NIC group, the interface that used the single NIC will use the NIC group.



CAUTION: Swapping NIC or NIC group parameters after you initially configure your firewall could have unexpected results.

Steps

- 1) Select **Network > Interfaces > NIC and NIC Group Configuration**. The **NIC and NIC Group Configuration** tab appears.



Tip: For option descriptions, click **Help**.

- 2) Select the two (and only two) NICs or NICs groups whose parameters you want to swap.
- 3) Click **Swap Parameters**.

View the interfaces that use a NIC or NIC group

View the interfaces and NIC groups that use a specific NIC or NIC group.

Steps

- 1) Select **Network > Interfaces > NIC and NIC Group Configuration**. The **NIC and NIC Group Configuration** tab appears.



Tip: For option descriptions, click **Help**.

- 2) Select the NIC or NIC group.
- 3) Click **Usage**.

Result

The **Usage** window appears listing the interfaces and NIC groups that use the NIC or NIC group.

Test connectivity for an interface or NIC

Use a ping test to check connectivity for an interface or NIC.

Steps

- 1) Select **Network > Interfaces**.
- 2) On the **Interface Configuration** tab or the **NIC and NIC Group Configuration** tab, click **Show Status**. The **Interface and NIC Status** window appears.

- 3) Click **Ping**. The **Ping Test** window appears.



Tip: For option descriptions, click **Help**.

- 4) In the **IP address** or **hostname** field, enter an IP address or fully qualified domain name (FQDN) that the ping will be sent to. To find the IP address for a host name, type the name, then click **DNS Lookup**.

- 5) [Optional] In the **Commandline flags** field, enter command line parameters for the ping test.



Tip: The **Commandline flags** field allows you to access additional functionality that would normally be available using the ping command. Run `man ping` on the command line.

- 6) Click **Start Ping**. The button changes to **Stop Ping**, and the ping results appear in the window.

- 7) To stop the test, click **Stop Ping**.

- 8) Click **Close**.

Quality of Service

Contents

- [Quality of Service and how it works](#) on page 397
- [QoS scenarios](#) on page 398
- [Configure Quality of Service](#) on page 400
- [Enable DSCP pass-through](#) on page 407

Quality of Service (QoS) guarantees a certain level of performance for a data flow by using different priorities and queuing mechanisms to allocate available bandwidth.

QoS is beneficial for networks with limited bandwidth that must pass latency-sensitive or bandwidth-intensive traffic.

Quality of Service and how it works

From the **Quality of Service** window, you can create and apply QoS profiles to a network interface.

Each QoS profile contains one or more queues that allow you to prioritize network performance based on network traffic type. All queues are assigned a priority value, allocated a percentage of available bandwidth, and allowed to borrow bandwidth from other queues. When a queue is full, any additional packets matching that queue are dropped. Queues are applied to network traffic based on the services selected.

When QoS policy is applied to a network interface, only outgoing traffic on that interface is controlled by QoS—packets arriving on that interface are not affected. If you require traffic for a particular service to be controlled in both directions, that service must be present in the QoS policy of both interfaces where traffic for that service leaves the firewall. Consider the following QoS configurations and their effect on a connection between an internal client and external web server.

- **External interface QoS profile includes HTTP** — Traffic sent from the internal client to the external web server is affected by QoS.
- **Internal interface QoS profile includes HTTP** — Traffic sent from the web server to the internal client is affected by QoS.
- **Internal and external interface QoS profiles include HTTP** — All traffic between the client and web server is affected by QoS.

QoS is applied to network traffic at the IP and transport layers based on the ports and protocols selected in each queue. Protocols that use dynamic ports negotiated at the application layer, like FTP or VoIP, will not match QoS queues using those services because QoS does not examine the application layer when processing packets.

Consider the case where a QoS queue has been created with the FTP proxy service selected. QoS is applied to the control connection (tcp port 21), but not the data connection (high random tcp port or tcp port 20). Since the control connection is made on the port defined in the QoS queue, QoS policy is applied to it. However, QoS is not applied to the data connection because it is made on a port negotiated at the application layer between the client and server.



Note: To apply QoS to protocols that employ dynamic ports, create a QoS queue that includes the range of dynamic ports.

QoS profile elements

QoS profiles contain QoS policy that can be assigned to a particular network interface. Profiles serve as containers for QoS queues that make up the QoS policy.

Each profile contains a default queue that cannot be deleted or renamed. The default queue processes all packets that do not match any queues you have explicitly defined.

QoS queues for the profile

Use QoS queues to allocate available bandwidth based on traffic type.

Queues make up the policy in QoS profiles. Each queue is assigned a priority value and dedicated a percentage of available bandwidth.

Each profile contains a default queue that cannot be deleted or renamed. The default queue processes all packets that do not match any queues you have explicitly defined.

Modify the **Priority**, **Bandwidth**, and **Can Borrow** attributes of the default queue to control how QoS allocates bandwidth for services that are not included in custom queues.

QoS policy creation

To create QoS policy, select the profile you want to modify in the **Profile** pane, then use the **Queue** pane to make policy changes.

To prioritize bandwidth usage within a profile, configure the attributes of each queue in the profile:

- **Priority** — A value between 0—7 (lowest—highest) that determines the order of queue processing relative to the other queues in the profile
Higher priority queues are processed first, resulting in lower latency for them.
- **Allocated Bandwidth** — The percentage of available bandwidth dedicated to the queue
The available bandwidth for a QoS profile is determined by the link speed of the network interface it is associated with.
- **Ports** — The types of traffic the queue applies to
- **Can Borrow** — If selected, allows the queue to borrow bandwidth from other queues in the profile when it exhausts its allocated bandwidth

QoS scenarios

The interaction between multiple QoS queues with differing priorities, allocated bandwidth, and borrowing can be complex.

Use these scenarios to familiarize yourself with QoS in practice. In these examples, two queues are configured—ssh and http. No other traffic is flowing, although other queues might be defined.

Scenario 1

At congestion levels, exactly 10% of available bandwidth is allocated to each of the queues.

- SSH is allocated 10% of bandwidth at priority 7 with no borrowing allowed.
- HTTP is allocated 10% of bandwidth at priority 7 with no borrowing allowed.

Scenario 2

At congestion levels, exactly 10% of available bandwidth is allocated to each of the queues. However, HTTP traffic is processed before SSH traffic; therefore, experiences lower latency.

- SSH is allocated 10% of bandwidth at priority 0 with no borrowing allowed.
- HTTP is allocated 10% of bandwidth at priority 7 with no borrowing allowed.

Scenario 3

At congestion levels, exactly 30% of available bandwidth is allotted to the SSH queue with 10% going to the HTTP queue.

- SSH is allocated 30% of bandwidth at priority 7 with no borrowing allowed.
- HTTP is allocated 10% of bandwidth at priority 7 with no borrowing allowed.

Scenario 4

At congestion levels, a proportionally larger percentage of available bandwidth is allotted to the SSH queue, with the remaining traffic going to the HTTP queue. Since SSH is allocated a larger portion of the bandwidth than HTTP, it gets more weight at the time of borrowing since they are of the same priority.

- SSH is allocated 30% of bandwidth at priority 7 with borrowing allowed.
- HTTP is allocated 10% of bandwidth at priority 7 with borrowing allowed.

Scenario 5

At congestion levels, the two queues share the borrowed bandwidth equally (40% each).

- SSH is allocated 10% of bandwidth at priority 7 with borrowing allowed.
- HTTP is allocated 10% of bandwidth at priority 7 with borrowing allowed.

Scenario 6

At congestion levels, the HTTP queue commandeers all of the bandwidth since it is the highest priority queue and is allowed to borrow.

- SSH is allocated 10% of bandwidth at priority 0 with borrowing allowed.
- HTTP is allocated 10% of bandwidth at priority 7 with borrowing allowed.

Scenario 7

At congestion levels, the SSH queue uses 30% of available bandwidth, and the HTTP queue commandeers all of the remaining bandwidth.

- SSH is allocated 30% of bandwidth at priority 7 with no borrowing allowed.
- HTTP is allocated 10% of bandwidth at priority 7 with borrowing allowed.

QoS summary

The firewall can handle queues in different ways depending on its configuration.

- If multiple queues have the same priority and borrowing is allowed, each queue borrows a percentage of available bandwidth. The amount of bandwidth each queue can borrow is determined by its allocated bandwidth in proportion to the allocated bandwidth of the other queues.
- If a queue with higher priority is allowed to borrow, it will starve lower priority queues, but not vice versa.
- If borrowing is not allowed, queues share available bandwidth per their allocated bandwidth value. Higher priority queues are serviced first, resulting in reduced latency for them at the expense of the lower priority queues.

Configure Quality of Service

Create QoS profiles and queues.



Note: QoS cannot be configured on VLANs.



Tip: Click **Load QoS Policy** to activate or reapply a QoS policy.

Create a QoS profile

Create a new QoS profile.

Steps

- 1) Select **Network > Quality of Service**. The **Quality of Service** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the Profile toolbar, click **New**. The **New Profile** window appears.

- 3) In the **Profile name** field, type a name for the new profile.



Note: The profile name must be between 1–7 characters.

- 4) [Optional] In the **Description** field, type a more detailed description of the profile.

- 5) Click **OK** to add the profile.

Modify QoS profiles

Change attributes of a QoS profile.

Edit a profile

Modify a QoS profile.

Steps

- 1) Select **Network > Quality of Service**. The **Quality of Service** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Profiles** pane, select a profile and click **Modify**. The **Modify Profile** window appears.

- 3) In the **Description** field, add a description or change the existing description.

- 4) Click **OK**.

Delete a profile

Delete a QoS profile.

Steps

- 1) Select **Network > Quality of Service**. The **Quality of Service** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Profiles** pane, select a profile and click **Delete**.

- 3) Click **Yes** to confirm the deletion of a profile.

Duplicate a profile

Duplicate a QoS profile.

Steps

- 1) Select **Network > Quality of Service**. The **Quality of Service** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Profiles** pane, select a profile and click **Duplicate**. The **New Profile** window appears.

- 3) In the **Profile name** field, type a name for the duplicate profile.

- 4) [Optional] In the **Description** field, type a detailed description of the profile.

- 5) Click **OK**.

Rename a profile

Rename a QoS profile.

Steps

- 1) Select **Network > Quality of Service**. The **Quality of Service** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Profiles** pane, select a profile and click **Rename**. The **Rename** window appears.

- 3) In the **New name** field, type a name for the profile.

- 4) Click **OK**.

Modify the simulated demand for a queue

Increase or decrease the simulated demand for a QoS queue.

Steps

- 1) Select **Network > Quality of Service**. The **Quality of Service** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Profiles** pane, select a profile.

- 3) Click **Simulate bandwidth allocation**.



Note: When the **Bandwidth Allocation Simulator** window opens, the simulated demand for each queue defaults to the percentage of bandwidth allocated to it.

- 4) Double-click the value in the **Simulated Demand** column.
- 5) Type the percentage demand you would like to simulate.
- 6) Press **Enter**.
- 7) Click **Close**.

Result

To simulate the worst case scenario where each queue is at 100% demand, click **Worst Case**.

Configure QoS queues for a profile

Create or modify a QoS queue for a profile.

Steps

- 1) Select **Network > Quality of Service**. The **Quality of Service** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Profiles** pane, select a profile.
- 3) From the **Queue** toolbar, click **New** to create a queue or select an existing queue, then click **Modify**.
- 4) In the **Name** field, type a name for the new queue. The name must be between 1–7 characters.



Tip: To rename an existing queue, click **Rename** on the queue toolbar.

- 5) [Optional] In the **Description** field, type a more detailed description of the queue.

- 6) In the **Priority** field, type the priority value for this queue.
- 7) In the **Bandwidth** field, type the percentage of bandwidth to be allocated for this queue.
- 8) Select the **Can borrow** checkbox to allow the queue to borrow bandwidth from the other queues.
- 9) In the **Ports** pane, configure the ports to associate with this queue.
 - **Select ports** — To select one or more ports, click **Port Lookup**.
 - To search for specific elements in the list, type your search criteria in the **Find** field. Clear this field to view the full list again.
 - Select the checkbox for each port to include, then click **OK**. The ports appear in the **Ports** pane.
 - **New** — To create a new port, click **New** on the **Ports** toolbar. The new port appears in the **Ports** pane.
 - **Modify** — To change a port:
 - In the **Port(s)** column, click the port. Type your change, then press **Enter**. The **Common Use** field displays updated information.
 - From the **Protocol** drop-down list, select the protocol for this port.
 - **Add or modify IP protocols** — To add entire IP protocols to the queue:
 - In the **Other IP protocols** field, type the number associated with one or more IP protocols using a comma-separated list.
 - Click **OK**.
 - **Delete** — To delete a port, select the port and click **Delete** on the toolbar.



Note: QoS queue policy is applied to packets that match the port and protocol.

- 10) Click **OK** to finish configuring the queue.




Note: Repeat this procedure for each additional queue you want to add or change for this profile.

Modify QoS queues

Change queue attributes.

Delete a queue

Delete a QoS queue.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Network > Quality of Service**. The **Quality of Service** window appears.
- 2) In the **Queues** pane, select a queue and click **Delete**.

- 3) Click **Yes** to confirm the deletion of a queue.



Note: You can't delete a default queue.

Rename a queue

Rename a QoS queue.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Network > Quality of Service**. The **Quality of Service** window appears.
- 2) In the **Queues** pane, select a queue and click **Rename**. The **Rename** window appears.
- 3) In the **New name** field, type a name for the queue.



Note: You can't rename a default queue.

- 4) Click **OK**.

Modify the priority or allocated bandwidth for a queue

Increase or decrease the priority or bandwidth for a QoS queue.

Steps

- 1) Select **Network > Quality of Service**. The **Quality of Service** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Queues** pane, select a queue.
- 3) Click **Update bandwidth**.
- 4) Double-click the value in the **Priority** or **Bandwidth** column that you wish to change.
- 5) Type the new value:
 - **Priority** — Type a value between 0–7 (lowest-highest).
 - **Bandwidth** — Type a value between 1–100 representing the percentage of bandwidth to allocate to this queue.
- 6) Press **Enter**.

- 7) Click **OK** and save your changes.



Note: The total allocated bandwidth cannot exceed 100 percent.

Apply the profile to a network interface

To complete the QoS configuration, apply the profile to a network interface.

Steps

- 1) Select **Network > Interfaces**. The **Interfaces** window appears.



Tip: For option descriptions, click **Help**.

- 2) Select the interface for this profile, then click **Modify** on the toolbar.
- 3) In the **Quality of Service** pane, use the drop-down list to select the QoS profile.




Tip: Click **New** to create a new QoS profile.

- 4) Click **OK**.

View QoS status

After configuring a QoS profile, view the QoS statistics.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Network > Quality of Service**. The **Quality of Service** window appears.
- 2) In the **Profiles** pane, select a profile.
- 3) Click **QoS status**. The **QoS Status** window appears.



Tip: Click **Refresh** to view the updated statistics.

- 4) Click **Close**.

Enable DSCP pass-through

You can allow Differentiated Services Code Point (DSCP) IP header information to be passed through TCP proxies.

While the firewall does not act on DSCP values, they are passed with Packet Filter. After passing through the firewall, other network devices can use the DSCP values for QoS traffic prioritization. You can enable this feature on TCP proxies, allowing those values to be preserved as the packet is processed. Both IPv4 and IPv6 addresses are supported.



Note: The default DSCP setting for TCP proxies is off.

If the DSCP value changes during a connection, the change might occur in a different data stream position after processing.

Example: If the DSCP value from the server starts as default, then changes to high priority after a few packets, the value sent to the client might not correspond. The change might briefly tag earlier data as high priority, or later data as default, but switches to high priority for the remainder of the connection.

These proxies are DSCP-capable:

- HTTP
- HTTPS
- FTP
- Generic TCP
- SMTP
- MSSQL
- SSH
- SOCKS

There are two ways to enable DSCP pass-through: from the command line or the File Editor.

Manage DSCP pass-through from the command line

To temporarily allow DSCP pass-through without having to restart the firewall, use the command line.



Note: If the firewall is in a cluster, these steps must be repeated on each firewall.

Steps

- 1) From the command line, log on to the firewall.
- 2) Type `srole` to change to the Admin domain.

- Choose the appropriate command.


Action	Command
Enable	<code>sysctl net.inet.tcp.dscp_proxy=1</code>
Disable	<code>sysctl net.inet.tcp.dscp_proxy=0</code>

Result

DSCP pass-through remains in effect until you restart the firewall. It then returns to the default setting.

Enable DSCP pass-through in the File Editor

To permanently allow DSCP pass-through, use the File Editor.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- Select **Maintenance > File Editor**.
- Click **Start File Editor**.
- Click **File**, then select **Open**.
- Select **Firewall File**.
- Type `/etc/sysctl.conf`, then click **OK**.
- Scroll to the end of the file.
- Add this line:

```
net.inet.tcp.dscp_proxy=1
```

- Save the file and exit.
Unless DSCP pass-through has been enabled from the command line, the DSCP change will take effect with the next restart of the firewall.

Result



Note: If the firewall is in a cluster, these steps must be repeated on each firewall.

DHCP Relay

Contents

- [How DHCP Relay helps](#) on page 409
- [Configure the DHCP Relay server](#) on page 409
- [Create DHCP Relay rules](#) on page 411

The Dynamic Host Configuration Protocol (DHCP) allows a server to dynamically assign IP address information to client hosts in a network.

Because DHCP clients request dynamic IP addresses using broadcast packets, DHCP clients and servers must typically reside in the same broadcast domain.

How DHCP Relay helps

The Dynamic Host Configuration Protocol (DHCP) allows a server to dynamically assign IP address information to client hosts in a network.

Because DHCP clients request dynamic IP addresses using broadcast packets, DHCP clients and servers must typically reside in the same broadcast domain.

The DHCP Relay feature allows the firewall to forward DHCP requests from clients to DHCP servers in different broadcast domains. To configure DHCP Relay, you must define the DHCP servers to forward requests to, and create policy rules to allow DHCP clients and servers to communicate with the DHCP Relay server on the firewall.



Note: DHCP Relay does not support IPv6.

Configure the DHCP Relay server

Define the destination and server options for the DHCP Relay server.

Define destination DHCP servers

The DHCP Relay server forwards DHCP requests to each DHCP server you define. If multiple servers respond to a DHCP request, the DHCP Relay server forwards the first response it receives to the client and ignores the others.

Define servers that DHCP requests are forwarded to.

Steps

- 1) Select **Policy > Network > DHCP Relay**. The **DHCP Servers** tab appears.



Tip: For option descriptions, click **Help**.

- 2) Add the servers to which DHCP requests should be forwarded.
 - a) Click **New**. The **New Server Address** window appears.
 - b) Enter the server's address information by doing one of the following:
 - Select **IP address**, then type the IP address of the server.
 - Select **Hostname**, then type the host name of the server.



Note: If you add a server using its host name, the firewall must be able to resolve the host name to an IP address using DNS.

- c) Click **Add**. You return to the **DHCP Servers** tab.
- 3) Save your changes.

Configure additional DHCP Relay server options

If needed, configure additional DHCP Relay server options.

Steps

- 1) Select **Policy > Network > DHCP Relay**, then click the **Advanced** tab.



Tip: For option descriptions, click **Help**.

- 2) Configure the advanced DHCP Relay server options as necessary.
- 3) Save your changes.

Create DHCP Relay rules

You must create policy rules to allow DHCP clients and servers to communicate with the DHCP Relay server on the firewall.

Steps

- 1) Select **Policy > Rules**.



Tip: For option descriptions, click **Help**.

- 2) Create a rule to accept DHCP requests from clients. Include these selections:
 - **Applications** — Select **DHCP Relay**.
 - **Source Zone** — Select the zone where the clients attempting to obtain IP addresses via DHCP are located.
 - **Source Endpoint** — Verify that **<Any>** is selected.
 - **Destination Zone** — Select the zone where the DHCP clients are located.
 - **Destination Endpoint** — Select or create an **IP Address** object with a value of **255.255.255.255**.



Note: The **Source Zone** and **Destination Zone** selections should be the same.

- 3) Create a rule to allow the DHCP server(s) to respond to DHCP requests. Include these selections:
 - **Applications** — Select **DHCP Relay**.
 - **Source Zone** — Select the zone or zones where the DHCP server(s) are located.
 - **Source Endpoint** — Restrict the source as desired, as long as the desired DHCP server(s) is included.
 - **Destination Zone** — Select the zone where the DHCP clients are located.
 - **Destination Endpoint** — Select or create an **IP Address** object for the IP address of the firewall in the zone where the DHCP clients are located.
- 4) [Conditional] Create a rule to allow clients to renew their DHCP leases from the DHCP server(s).



Note: Some DHCP clients, such as Windows XP computers, attempt to renew their DHCP address leases by directly connecting to the DHCP server that assigned addresses to them. If your network environment requires that this be allowed, complete this step.

Include these selections:

- **Applications** — Select **DHCP Relay**.
 - **Source Zone** — Select the zone where the DHCP clients are located.
 - **Source Endpoint** — Restrict the source as desired, as long as the desired DHCP clients are included.
 - **Destination Zone** — Select the zone or zones where the DHCP server(s) are located.
 - **Destination Endpoint** — Restrict the destination as desired, as long as the desired DHCP server(s) are included.
- 5) Make sure that the rules you created in *Step 2* through *Step 4* are enabled and above the **Deny All** rule.
 - 6) Save your changes.

Routing

Contents

- [Routing protocols in firewall](#) on page 413
- [Configuring static routes](#) on page 414
- [Configuring dynamic routing server processing](#) on page 419
- [What RIP does](#) on page 420
- [How OSPF works](#) on page 429
- [Concepts of OSPF IPv6](#) on page 434
- [What BGP passes](#) on page 437
- [Why the PIM-SM protocol is used](#) on page 443
- [Dynamic routing in HA clusters](#) on page 456
- [Troubleshooting dynamic routing issues](#) on page 456

Traffic between machines on different networks or subnets requires routing. This routing information can be input manually using *static routes* and learned automatically using *dynamic routing*.

Routing protocols in firewall

Each computer in your network also designates a specific route as its default route, to use when the computer cannot find an explicit route to the destination.

This default gateway is generally a router that allows access to distant subnets. You can configure an alternate default route to act as a redundant route. If your primary default route becomes inaccessible, an alternate default route begins forwarding traffic.

The Sidewinder can participate in routing using information from static routes, and can act as a default gateway for your network.

The firewall supports four dynamic routing protocols:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF) protocol
- OSPF IPv6 protocol
- Border Gateway Protocol (BGP)
- Protocol Independent Multicast - Sparse Mode (PIM-SM) protocol

This chapter provides a brief overview of how each protocol works, and guidelines and scenarios for configuring the dynamic routing protocols and servers on the Sidewinder. The Sidewinder implementation of these protocols and their respective servers are based on the Quagga implementation. Any administrator planning on configuring RIP, OSPF, BGP, or PIM-SM on a Sidewinder is strongly encouraged to use the online help that is available when connected to a Sidewinder-hosted routing server using a command line interface, and the Quagga documentation available at <http://www.nongnu.org/quagga/docs.html>.

Configuring static routes

Static routes are based on a fixed forwarding path.


To create and modify static routes, select **Network > Routing > Static Routing**. The **Static Routing** window appears.

The table lists static routes configured on this firewall. **Primary Default** and **Alternate Default** appear automatically in the table. If IPv6 is enabled on the firewall, **IPv6 Default** also appears.

- The primary default route is created when you initially configure the firewall.
- The alternate default route is a placeholder. You must configure the alternate default route to enable default route failover.

Use the toolbar to perform these actions:

Table 83: Static Routing Options

Button	Action
New	Create a static route by clicking New and entering information in the Host/Network Route Properties pop-up window.
Modify	<ul style="list-style-type: none"> • Modify the default route by selecting Primary Default and clicking Modify. Modify the single static default route settings in the Default Route Properties pop-up window. • Configure default route failover by selecting Primary Default or Alternate Default and clicking Modify. Configure the primary and alternate default routes in the Default Route Properties pop-up window. • Modify an existing static route by selecting it and clicking Modify. Modify the settings in the Host/Network Route Properties pop-up window.
Delete	Delete a static route by selecting it and clicking Delete . <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;">  Note: The values of the primary and alternate default routes are deleted. The placeholders for the default routes remain in the table. </div>
Find	Search for a specific element(s) in the list using the Find field. Type your search criteria, and routes with matching elements will appear in the list. Clear this field to see the full list again.
Status	To view the status information of the routes configured for the firewall, click Status . You can also view route failover status and route failover audit, and you can reset the default route when it becomes accessible.

Related concepts

[Checking route status and reset the default route](#) on page 418

Related tasks

[Configure default routes](#) on page 415

[Configure other static routes](#) on page 418

Configure default routes

Use the **Default Route Properties** window to modify details for the default routes.

Modify the primary default route

Change the attributes of the primary default route.

Steps

- 1) Select **Use single static default route**.



Tip: For option descriptions, click **Help**.

- 2) In the **IP address** field, enter the address of the device the firewall forwards traffic to if there is no known route for the destination address. This is usually the IP address of a device that forwards packets to your Internet Service Provider.
 - To find the IP address for a host name, enter the host name in the field and click **DNS Lookup**.
 - To return the IP address to the currently configured default route, click **Use current default route value**.
- 3) [Optional] In the **Description** field, enter information that will help identify the route in the **Static Routing** window.
- 4) Click **OK** and save your changes.



Note: If you have a DHCP interface configured and enabled, the default route is assigned dynamically. The dynamic address supersedes a single static default route configured in this window. The dynamically assigned default route appears in the read-only **Current default route** field. Click **Refresh** to update this field.

Configure default route failover

To configure redundant default routes, you define an alternate default route and ping addresses for the default routes.

- Sidewinder continuously pings the default route IP address and any other ping addresses that you define.
- If all configured ping addresses fail, the alternate default route becomes the acting default route.
- Use the **Static Route Status** window to reset the primary default route when it is active again.

The current default route is shown in a read-only field. Click **Refresh** to update this field.

Steps

- 1) Select **Use alternate default routes**.



Tip: For option descriptions, click **Help**.

- 2) [Optional] Configure the primary default route IP address. The currently configured default route information appears automatically.
 - In the **IP address** field, enter the address of the device the firewall forwards traffic to if there is no known route for the destination address. This is usually the IP address of a device that forwards packets to your Internet Service Provider.
 - To find the IP address for a host name, enter the host name in the field and click **DNS Lookup**.
 - To return the IP address to the currently active default route, click **Use current default route value**.
 - To use dynamic addressing for the primary default route, type `dhcp`. You must have a DHCP interface enabled.
 - In the **Description** field, enter information that will help identify the route in the **Static Routing** window.
- 3) [Optional] In the **Ping addresses** area, configure the IP addresses that the firewall will ping to confirm that the primary default route is accessible.

The primary default route IP address appears automatically. We recommend using an IP address upstream from the primary default route.

To configure additional ping addresses:

- a) Click **New**, then click the **Specify IP Address** field and type an IP address that the firewall will ping.
- b) In the **Ping interval** field, specify how often (in seconds) the firewall will ping the configured IP addresses to ensure that the path is accessible.
- c) In the **Failures allowed** field, specify the number of failed ping attempts that must occur before the alternate default route takes over as the primary.

Failures are counted in increments and decrements rather than successively. This means that a failed ping adds to the failure total, and a successful ping subtracts from the failure total. The failure total is never less than zero and it is never more than the configured failures allowed.

For example, if the configured failures allowed is **3**, this is how the failure count is tallied based on the ping results:

Table 84: Sample failed ping attempt tally

Ping result:	failure	success	success	failure	failure	success	failure	failure	Failover event occurs
Failure total:	1	0	0	1	2	1	2	3	

To modify a ping IP address, double-click the address in the list and make the change.

To delete a ping IP address, select it in the list and click **Delete**.

- 4) Configure the alternate default route IP address.
 - In the **IP address** field, enter the address of the device the firewall forwards traffic to if there is no known route for the destination address. This should be a different route than the primary default route, or to a different ISP.
 - To find the IP address for a host name, enter the host name in the field and click **DNS Lookup**.
 - To return the IP address to the currently active default route, click **Use current default route value**.
 - To use dynamic addressing for the alternate default route, type `dhcp`. You must have a DHCP interface enabled.
 - In the **Description** field, enter information that will help identify the route in the **Static Routing** window.
- 5) In the **Ping addresses** area, configure the IP addresses that the firewall will ping to confirm that the alternate default route is accessible.
 - a) Click **New**, then click the **Specify IP Address** field and type an IP address that the firewall will ping. We recommend using an IP address upstream from the alternate default route.
 - b) In the **Ping interval** field, specify how often (in seconds) the firewall will ping the configured IP addresses to ensure that the path is accessible.
 - c) In the **Failures allowed** field, specify the number of failed ping attempts that must occur before the alternate default route is considered inaccessible.

Failures are counted in increments and decrements rather than successively. This means that a failed ping adds to the failure total, and a successful ping subtracts from the failure total. The failure total is never less than zero and it is never more than the configured failures allowed.

For example, if the configured failures allowed is **3**, this is how the failure count is tallied based on the ping results:

Table 85: Sample failed ping attempt tally for the alternate default route

Ping result:	failure	success	success	failure	failure	success	failure	failure	Alternate stops forwarding
Failure total:	1	0	0	1	2	1	2	3	

To modify a ping IP address, double-click the address in the list and make the change.

To delete a ping IP address, select it in the list and click **Delete**.

- 6) Click **OK** and save your changes.

Configure the IPv6 default route

Configure a default using an IPv6 address.

Steps

- 1) In the **IP address** field, enter the address of the device the firewall forwards traffic to if there is no known route for the destination address.

This is usually the IP address of a device that forwards packets to your Internet Service Provider. To find the IP address for a host name, enter the host name in the field and click **DNS Lookup**.



Tip: For option descriptions, click **Help**.

- 2) [Optional] In the **Description** field, enter information that will help identify the route in the **Static Routing** window.
- 3) [Conditional] If the static route is a link-local address (begins with *fe80*), you must select an interface from the **Interface** drop-down list.
- 4) Click **OK** and save your changes.

Checking route status and reset the default route

The **Static Route Status** window enables you to check for the status of a route and also allows you to reset a default route.

Configure other static routes

Configure additional static routes.

Steps

- 1) Select the route type:
 - **Host** — Select this option if your destination is a specific IP address.
 - **Network** — Select this option if your destination is a network.



Tip: For option descriptions, click **Help**.

- 2) In the **Description** field, enter information that will help identify the route in the **Static Routing** window.
- 3) In the **Destination** field, enter the host IP address or subnet address of your end target. To find the IP address for a host name, enter the host name in the field and click **DNS Lookup**.
- 4) [Network only] Make the appropriate entry.
 - For an IPv4 address, in the **Prefix** field, type the network mask that will be used for this route.

- For an IPv6 address, in the **Prefix** field, enter the mask length. Valid values are 0–128
- 5) In the **Gateway** field, type the gateway address that the route will use to pass traffic on to the destination. The gateway address must be reachable by the Sidewinder.
To find the IP address for a host name, enter the host name in the field and click **DNS Lookup**.
 - 6) [Optional] In the **Distance** field, enter the rank for this route. Valid values are 1–254.
 - 7) [Conditional] If an IPv6 static route is a link-local address (begins with *fe80*), you must enter a valid interface in the **Interface** field.
 - 8) Click **OK** and save your changes.

Configuring dynamic routing server processing

Sidewinder offers an administrative version of the dynamic routing server configuration files to improve dynamic routing management.

The administrative configuration file maps the appliance interface name to the Network Interface Card (NIC) name. This ensures that the correct NIC is referenced if there are High Availability (HA) cluster members with different interface-to-NIC mappings or if the NIC hardware is replaced and the NIC name changes. The administrative and agent configuration files must be synchronized.

We recommend using one of the following methods to configure dynamic routing server processing because the synchronization of the administrative and agent configuration files occurs automatically:

- Use Telnet to connect to the dynamic routing server Quagga VTY shell (command line interface method) on the firewall.
- Use the Admin Console dynamic routing configuration file editors located under **Network > Routing > Dynamic Routing** to edit the dynamic routing server configuration file.



Note: In an HA cluster, configure dynamic routing only on the primary firewall. Dynamic routing information is automatically synchronized with the secondary firewall.

Specifying network information

The network information you specify depends on the method you use to configure dynamic routing server processing.

Specify network information as follows:

- **NIC names** — If using the command line interface method
- **Interface names** — If using the Sidewinder Admin Console dynamic routing configuration file editors, a different file editor such as *vi*, or the Control Center user interface

Configure dynamic routing server processing using a file editor

If you do not use the Admin Console File Editor, but another file editor, such as `vi`, to edit the dynamic routing server configuration file, you must perform the file synchronization manually.

Steps

- 1) Edit the administrative configuration file for the appropriate dynamic routing server. The administrative configuration files are located in the `/secureos/etc/quagga` directory and are prefixed with `admin_`.
- 2) To synchronize the administrative and agent configuration files, enter the following command:

```
cf route export agent=bgpd/ospfd/ospf6d/ripd/zebra zone=ripzone
```



Note: The zone only applies if using RIP bound to a zone.

What RIP does

The Routing Information Protocol (RIP) passes dynamic routing information to be used by routers and servers performing routing functions.

A router passing RIP traffic can be configured to receive routing information, install routes in its local routing table, and advertise routing information. A router uses this information to determine the shortest available path between networks. By default, routing information is exchanged every 30 seconds and when a router receives updates.



Note: IPv6 is not supported for RIP on Sidewinder.

RIP processing is performed by a Sidewinder routing server. The routing server operates by listening for UDP broadcasts on port 520. It sets a timer to send a RIP packet advertising its routing information every 30 seconds. When a RIP broadcast is received, the routing server updates the local routing table with any new routes. When the 30 second timer expires, the routing server reads and updates its local routing table, and then advertises its local routing information.

The routing server has two implementations:

- RIP Unbound Server — Automatically broadcasts routing information to all zones. This is the recommended method.
- RIP Routing Server — Learns routes without broadcasting routing information



Note: Only one RIP routing method can be enabled in a zone.

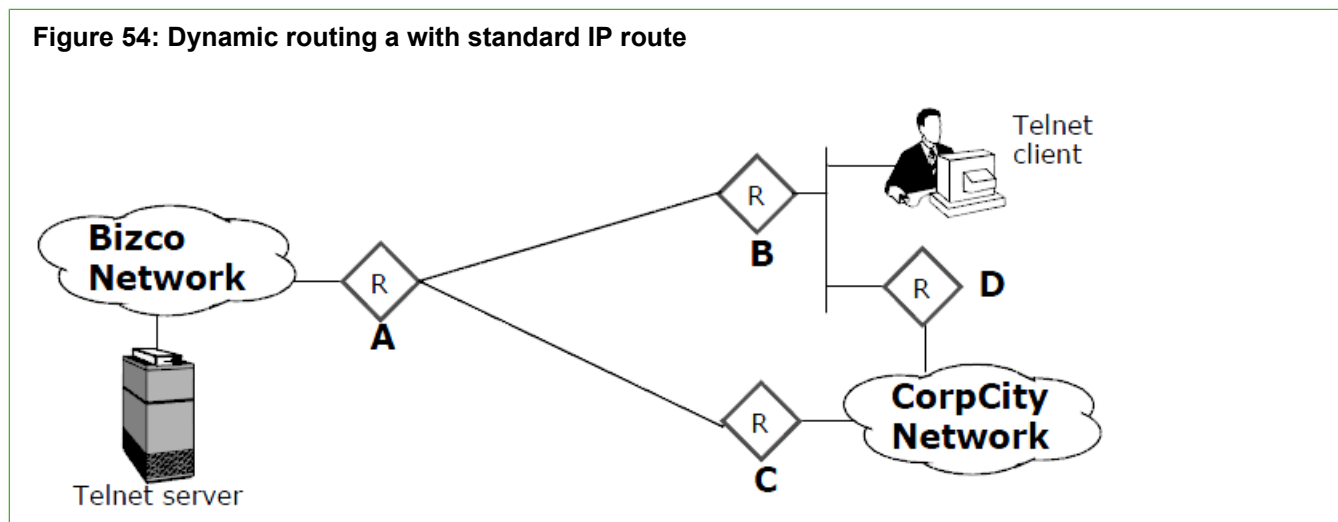
The following sections contain scenarios that explain the general concept of RIP processing, some considerations when using RIP on a single zone, and some considerations when using RIP on multiple zones.



Attention: In general, dynamic routing is less secure than static routing. If your network requires dynamic routing using RIP, we recommend using RIP v2, which is more secure than RIP v1 and also offers authentication. By default, the RIP Routing Server and RIP Unbound Server use v2 without authentication. See the Quagga documentation for enabling authentication.

This example describes how RIP processing aids in routing IP packets through a network that has a redundant routing architecture. The following figure illustrates this redundant architecture.

Figure 54: Dynamic routing a with standard IP route



In this example, the Telnet server has a static route to router A, and the Telnet client has a static route to router B. The Telnet client has two different possible paths of reaching the server: (1) via B to A, and (2) via D to C to A. The routing table on router B has two possible routes to the Bizco network: one with a hop count equal to two (through router A), and the other with a hop count to three (through router D). All routers are using RIP to advertise, create, and receive routing information from the other routers.

Typically, when the Telnet client needs to connect to the Telnet server, it sends a connection request to router B (the client's default route). B then forwards the request to router A, because that is the shortest route (two hops versus three hops). Router A then forwards the request to the Telnet server in the Bizco network, which uses the same route to respond to the request.

The dynamic routing capability of RIP can be seen when the link between router A and router B is lost. As soon as B notices that it is no longer receiving RIP updates from A, it updates its local routing table hop count for that route to 16 (route unreachable) and broadcasts this to others on its local network (this is to notify router D).

Next, the Telnet client sends another packet to the server via router A, unaware that the route between A and B has been lost. Router B looks at its local routing table and discovers there are two routes: one is unreachable and the other goes through router D. Because D is on the same network as the client, router B sends an ICMP Redirect back at the client stating that it can reach the Telnet server network through router D. The client updates its local routing table to point that host at router D. The client then re-sends its last packet to router D. Router D receives the packet and forwards it on to router C, which forwards it on to router A, and so on. The session continues on through router D without interruption. When the link between A and B is re-established, the Telnet client will receive an ICMP Redirect from router D pointing it back at router B. The session will again continue without interruption.

Related concepts

[Configuring RIP](#) on page 421

Configuring RIP

To implement RIP processing, a RIP Routing Server process must be configured and there must be an active rule that allows RIP broadcasts.

The RIP Routing Server is then enabled in that rule's source zone for the RIP Routing Server bound to a zone, or multiple zones for the RIP Unbound Server. RIP packets are UDP datagrams with destination port 520. For RIP version 1, the destination address is a network broadcast address such as 10.10.10.255. For RIP version 2,

all the routers multicast the address 224.0.0.9. Each zone will have no more than a single RIP Routing Server instance to handle the network traffic for all interfaces assigned to the zone.

These are the high level steps to set up RIP on the Sidewinder.

- 1) Sketch a diagram showing your planned Sidewinder configuration. Include the following items on your diagram:
 - configuration of the routers to which the firewall connects
 - RIP network
 - the Sidewinder interfaces (zones)
- 2) Define one or more netgroups for the routers to which the firewall connects.
- 3) Configure one or more rules for the RIP traffic.
- 4) Configure the appropriate RIP parameters.

See the following sections for details on these high level steps.

Using RIP in your network is a two-step process: First you must create a rule that allows the RIP Routing Server to pass traffic. Then you must configure the RIP Routing Server with the appropriate network information and processing options.

Related concepts

[What RIP does](#) on page 420

[RIP processing options](#) on page 425

Related tasks

[Create a rule for the RIP Unbound Server](#) on page 422

[Manage network objects](#) on page 86

Create a rule for the RIP Unbound Server

To pass RIP traffic in more than one zone, you must run the same server instance in more than one zone. To do this, configure the RIP Unbound Server.

Create a rule using the RIP Unbound Server; using the RIP Unbound Server in an enabled rule automatically enables the RIP Unbound Server in the rule's source zone. (You cannot access the RIP Unbound Server configuration files using the command line interface until this rule is created and enabled.) You can disable the server by disabling or deleting all rules that use the RIP Unbound Server, and by disabling the RIP Unbound Server in its configuration file.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the new rule.

- 4) In the **Application** field, select **RIP Unbound Server**.
- 5) Configure the **Source** and **Destination** fields as necessary to enforce your RIP security policy.



Note: The same zone cannot be used in both a rule using the RIP Unbound Server and a rule using the RIP Routing Server.

- 6) Save your changes.

Create a rule for RIP Routing Server bound to a zone

To pass RIP traffic bound to a zone, the firewall needs a rule with the Application field set to RIP Routing Server. The source and destination zones must be the same, and should be set to the zone on which you intend to receive RIP packets.

The source endpoint represents who you want to accept RIP traffic from, such as a single router or a netgroup of routers and/or hosts. The destination endpoint will usually be set to **Any**, since the destination is the broadcast address that corresponds to the source and destination zone.

Using the RIP Routing Server in an enabled rule automatically enables the RIP Routing Server in the rule's source zone. (You cannot access the RIP Routing Server configuration files using the command line interface until this rule is created and enabled.) You can disable the server by disabling or deleting all rules that use the RIP Routing Server, and by disabling the RIP Routing Server in its configuration file.



Note: Use of the RIP Routing Server binds the server to a single zone. Since no routes can be shared between RIP Routing Servers, the RIP Routing Server learns routes only in that zone.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the new rule.
- 4) In the **Application** field, select **RIP Routing Server**.
- 5) Set the **Source Zone** and the **Destination Zone** fields to the same zone. This enables the RIP Routing Server in that zone.
 - The same zone cannot be used in both a rule using the RIP Unbound Server and a rule using the RIP Routing Server.
 - You can enable the RIP Routing Server in multiple zones. There is one configuration file per zone, and each file must be edited separately.
- 6) Configure the other **Source** and **Destination** fields as necessary to enforce your RIP security policy.
- 7) Save your changes.

Result

For the firewall to pass RIP traffic, you now need to configure the RIP Routing Server configuration file with the settings appropriate for your security policy. See the following section for the preferred method for enabling and disabling the RIP Routing Server.

Configure basic RIP Routing Server processing

There are several ways to configure the RIP Routing Server on the Sidewinder.

- Using Telnet to connect to the RIP Routing Server on the firewall.
- Using the Admin Console File Editor to edit the RIP Routing Server configuration file.
- Using a different file editor, such as vi, to edit the RIP Routing Server configuration file.

Because the command line method provides RIP Routing Server help and validates commands as they are entered, the following sections focus on this method. The same commands and functionality described here are valid when using the other methods, but require different formatting. Be sure that you are familiar with RIP Routing Server formatting conventions before using those methods.

For additional documentation on RIP processing, see the official Quagga web site at <http://www.nongnu.org/quagga/docs.html>.

Steps

1) Using a command line session, log on to the firewall and switch to the Admn domain by entering:

```
srole
```

2) Telnet into the Sidewinder RIP Routing Server on localhost by entering the appropriate command:

- `unbound — telnet localhost ripd`
- `bound to zone — telnet localhost_n ripd`

where *n* = the zone index of the zone used as the source zone in the enabled RIP Routing Server access control rule.



Tip: Use `cf zone query` to look up a zone's index. It is also listed on the **Network > Zone Configuration** window as the ID.

A password prompt appears.

3) Enter `zebra`.

A `ripd>` prompt appears.

4) Enable the full command set by entering:

```
ripd>en
```

The prompt changes to `ripd#` to indicate that the full command set is enabled.

5) Enable configuration mode by entering:

```
(config)#conf t
```

The prompt changes to `ripd(conf)#` to indicate that configuration mode is enabled.

- 6) Enable the RIP Routing Server and configure it to advertise routes, receive updates, and install routes in the local routing table by entering the following commands:

```
(config)#router rip
(config-router)#network X.X.X.X/mask
```

where *X.X.X.X/mask* is the subnet and network mask of the interface on which you are enabling RIP. You can enter multiple network statements.

- 7) [Optional] To make changes persistent across restarts, write the changes to the configuration file by entering:

```
(config)#write
```

Result

The RIP Routing Server is now enabled and is sending, receiving, and creating routing information. See the following section for information on other configuration options.

To disable the RIP Routing Server, follow *Step 1* through *Step 5* in the previous procedure, and then enter:

```
(config)#no router rip
```

The RIP Routing Server is now disabled and will not participating in routing.

RIP processing options

The following is a list of common RIP configurations and the commands to implement these configurations. Only administrators who are experienced with routing in general, and RIP dynamic routing in particular, should configure the RIP Routing Server.

These commands are presented as they are entered at a command line interface. They also assume that you have entered the appropriate network statements when you first accessed the RIP Routing Server. Another option is to configure these options by using the Admin Console File Editor or other file editor to edit the configuration file directly. If you chose to modify the file directly, pay close attention to formatting. See the Quagga documentation at <http://www.nongnu.org/quagga/docs.html> for formatting assistance.



Tip: Use the RIP Routing Server online help, available when using the CLI, for details on modifying the commands given here as well as other supported configurations. To access the RIP Routing Server online help, enter a mode (such as `router rip` or `route-map`) and then enter `?` or `list`. You must be currently running a mode to see its documentation.

- **Receive and create routes, but do not advertise routes**

This configuration enables RIP on all interfaces that are on the specified subnet. In this option, the RIP Routing Server receives updates and creates routes in the local routing table, but does not advertise routes. Use these commands to configure this option:

```
(config)#router rip
(config-router)#passive-interface if_name
```

where *if_name* is the interface name of the zone that is to learn routes, but does not advertise routes. Use `default` instead of an interface name to set this configuration on all interfaces.

- **Advertise routing information, but do not receive or create routes**

This configuration enables the RIP Routing Server to send RIP updates that advertise local routing information available within the current zone. RIP ignores received updates and does not create routes in the local routing table. Use these command to configure this option:

```
(config)#ip prefix-list name seq n deny x.x.x.x/mask
(config)#router rip
```

```
(config-router)#distribute-list prefix name in|out
```

where:

- *name* is the name of the prefix-list
- *n* indicates the order of the prefix-list. Sequence numbers are generally multiples of 5.
- *x.x.x.x/mask* is the IP address and netmask that identified the route. To include all routes, use *any*.
- use *in* to filter routes received by this zone and *out* to filter routes sent by this zone.

For example, you would create an `ip prefix-list` named `none` with a seq 5 that denies all routes. The second command uses `distribute-list` to filter out all received (inbound) updates.

- **Advertise as the default route**

This configuration enables the RIP Routing Server to advertise the default route prefix.

Use this command to configure this option:

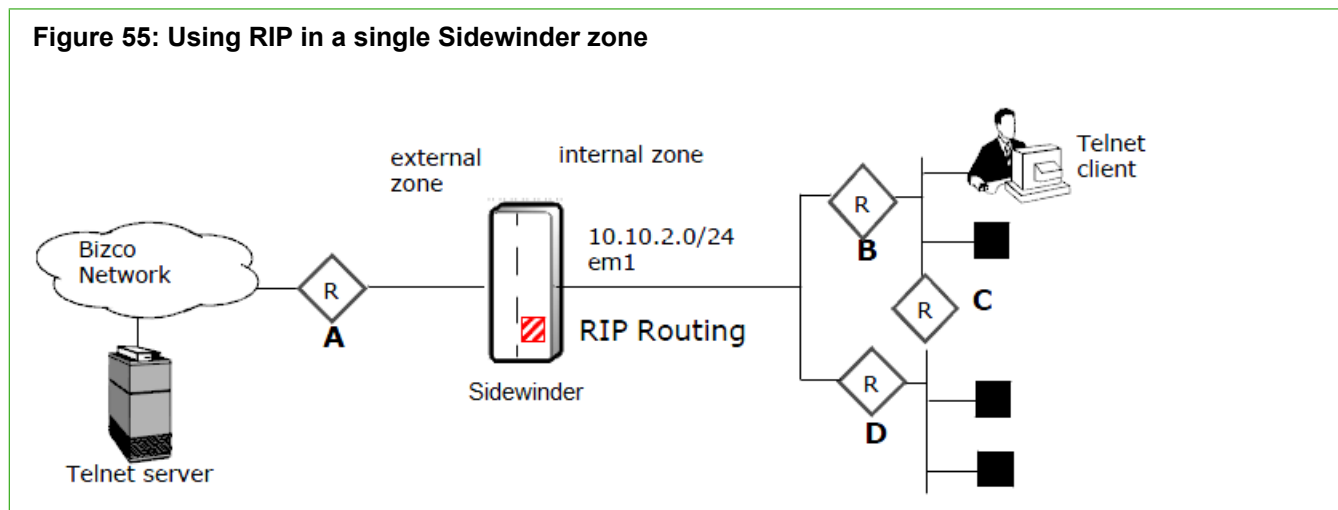
```
(config)#router rip
```

```
(config-router)#default-information originate
```

Enabling the RIP Routing Server on a single Sidewinder zone

A simple implementation of RIP on the Sidewinder is to enable the RIP Routing Server in a single zone.

This configuration is useful when the firewall has a zone that is connected to a network with a redundant routing topology and the firewall needs to participate in that routing infrastructure, but does not need to share that information with other zones.



In this scenario, the company security policy calls for the RIP Routing Server to participate in dynamic routing internally without sharing routing information with any other zones. To achieve this goal, an administrator enables the RIP Routing Server on the internal zone. If any of the internal routers (B, C, or D) becomes unreachable, the RIP Routing Server receives this information, updates its routing table accordingly, and then advertises the change. For example, if the Telnet client was using router B and it goes down, the client's host machine gets an update for the Sidewinder RIP Routing Server and reroutes its request through router C and D. When router B is available, the client's host machine receives that update and begins using router B again. On the external zone, the firewall maintains a static route with router A.

To implement this policy, the administrator configures the following RIP Routing Server options on the *internal zone*:

- Advertise routing information to the internal zone
- Distribute a default route
- Receive routing information from other routers on the internal zone
- Does not send or receive information from any other zones

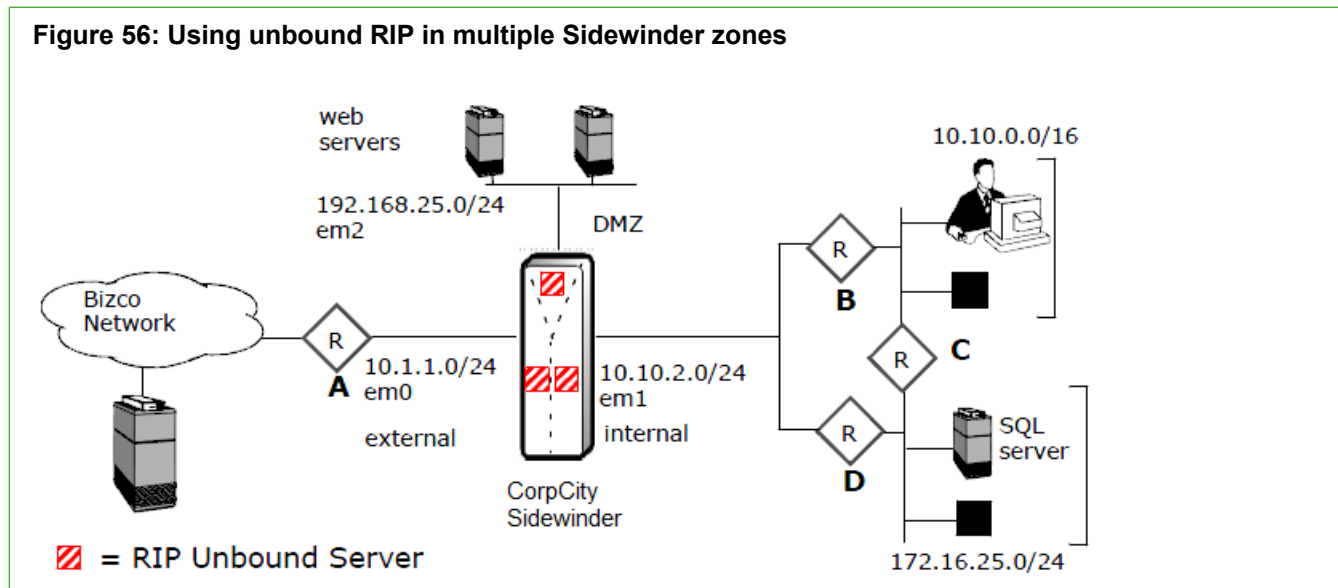
The configuration file for this policy would be similar to the following:

```
!ripd.conf.internal for internal zone
router rip
network 10.10.2.0/24
default-information originate
```

Enabling RIP processing on multiple Sidewinder zones

Using the RIP Unbound Server in multiple Sidewinder zones involves more options than using it in a single zone. You can make decisions about what information to share and what information to filter out.

Figure 56: Using unbound RIP in multiple Sidewinder zones



In this scenario, the company security policy calls for using unbound RIP to share routing information between the external zone and the DMZ zone, while passing routing information from the internal zone. The administrator must configure the RIP Unbound Server to pass routing information between the DMZ and the external zone, and advertise the subnet containing the company’s SQL servers, but filter out the routing information for the subnet hosting the employees computers.

To implement this policy, the administrator configures the RIP Unbound Server for the external zone and the DMZ zone to share all information, but only advertise the SQL subnet information from the internal zone.

The configuration file for the external zone and the DMZ zone would be similar to the following:

```
!ripd.conf for dmz and internal zone
router rip#
network 196.168.25.0/24
network 10.1.1.0/24
route 172.16.25.0/24
```

The administrator then configures the RIP Routing Server with these options on the internal zone:

- Advertise routing information within the internal zone

- Distribute a default route to the internal zone

The configuration file for this RIP Routing Server policy would be similar to the following:

```
!ripd.conf.internal for internal zone router rip
  network 10.10.2.0/24
default-information originate
```

Viewing and comparing RIP Routing Server configurations

The Admin Console provides tools to help you manage your RIP configuration. You can use these tools to quickly view the entire configuration file, compare different states of the configuration file, or list items such as the RIP neighbors and routes.

You can also use the RIP area to edit the configuration file using the File Editor and to manually overwrite the configuration to be used the next time the RIP Routing Server restarts.

To use these tools, select **Network > Routing > Dynamic Routing > RIP**

On this window, you can do the following:

- **Determine which configuration file to view and edit** — The unbound RIP option and each zone have a separate configuration file. Select an option from the **Zone** drop-down list to determine which configuration file to manage.



Note: In addition to editing a RIP Routing Server configuration file, you must create a rule before RIP traffic can be passed.

- **Edit a configuration file** — Click **Edit** to open the selected zone's configuration file using the Admin Console File Editor. Edit the file as needed and then save your changes. The firewall automatically restarts the RIP Routing Server.
- **View and compare files** — Select an option from the list and then click **Retrieve**. A pop-up window appears displaying the requested information. Close this pop-up to return to the main RIP window.
- **Save the running configuration to the configuration file** — Click **Overwrite** to save the running configuration. The running configuration and the starting configuration are now the same.

Related concepts

[Configuring RIP](#) on page 421

Related tasks

[Create a rule for the RIP Unbound Server](#) on page 422

[Create a rule for RIP Routing Server bound to a zone](#) on page 423

How OSPF works

The Open Shortest Path First (OSPF) protocol passes link-state information about the internal routers in a given network. All routers communicating using OSPF use an algorithm to calculate the shortest path among the routers.

On the Sidewinder, OSPF processing is performed by the Sidewinder OSPF Routing Server. To implement OSPF processing, the OSPF Routing Server must be configured and there must be an active rule that allows OSPF broadcasts. Unlike RIP which is zone-specific, the OSPF Routing Server automatically advertises its routing information to all zones on the firewall. OSPF runs as its own protocol (protocol 89) at the IP layer. OSPF uses 224.0.0.5 and 224.0.0.6 as multicast addresses.

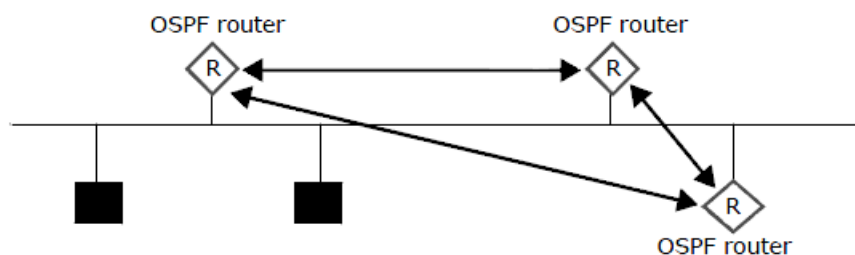
OSPF multicasts information frequently. When a host detects a change to a routing table or a change in the network topology, it immediately multicasts the information to all other hosts in the network. Unlike the RIP in which the entire routing table is sent, the host using OSPF sends only the part that has changed. With RIP, the routing table is sent to neighboring hosts every 30 seconds. OSPF multicasts updated information only when a change occurs.

Rather than counting the number of hops, OSPF bases its path descriptions on link states that factor in additional network information. Also, OSPF lets you assign cost metrics to a given host router so that some paths are given preference.

There are three phases to the OSPF protocol:

- 1) Routers discover neighboring OSPF routers by exchanging Hello messages. The Hello messages also determine which routers are to act as the *Designated Router (DR)* and *Backup Designated Router (BDR)*. These messages are exchanged periodically to ensure connectivity between neighbors still exists.
- 2) Routers exchange their *link state databases*. *Link state* means the information about a system's interfaces, such as its IP address, network mask, the cost for using that interface, and whether it is up or down.
- 3) The routers exchange additional information via a number of different type of *Link State Advertisements (LSAs)*. These supply the information needed to calculate routes. Some reasons for generating LSAs are interfaces going up or down, distant routes changing, static routes being added or deleted, etc.

Figure 57: Three OSPF protocol phases



- a. Exchange Hello messages to discover neighbor OSPF routers
- b. Exchange link state databases
- c. Exchange link state advertisements

At this point, all routers should have a full database. Each database contains consistent (not identical) information about the network. Based upon this information, routes are calculated via the “Dijkstra” algorithm. This algorithm generates the set of shortest routes needed to traverse the network. These routes are then enabled for use by IP.

All OSPF routers on a network do not exchange OSPF data—this limits network overhead. Instead, they communicate with the DR (and BDR), which are then responsible for updating all other routers on the network.

Election of the DR is based upon the priority of that router. OSPF multicasts using the *AllSPFRouters* (224.0.0.5) and *AllDRouters* (224.0.0.6) addresses. The DR and the BDR receive packets on the second address.



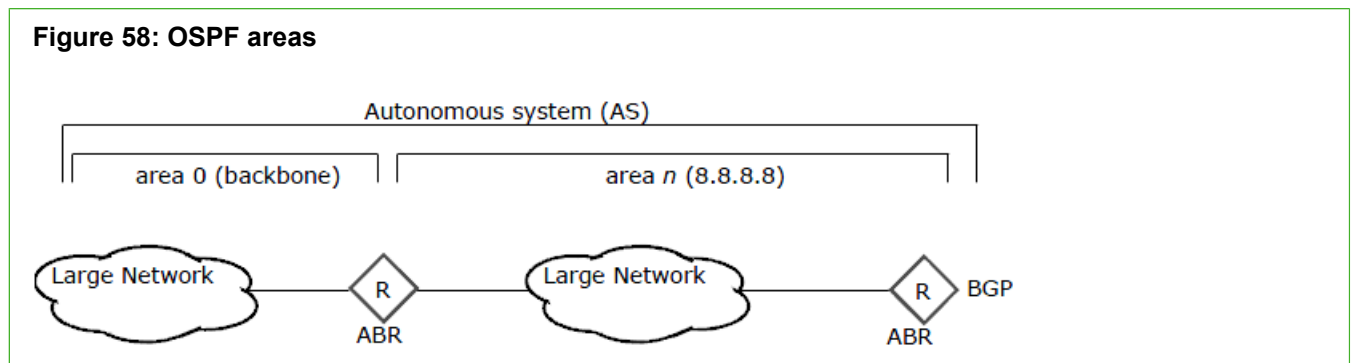
Note: Since the Sidewinder performs many other functions, we recommend that customers should not configure the firewall to become DR (or BDR) unless forced to by network topology.

OSPF is considered an Interior Gateway Protocol (IGP). An IGP limits the exchange of routes to a domain of control, known as an Autonomous System (AS). An AS is a large network created under a central authority running a consistent routing policy that includes different routing protocols, such as the networks commonly run by ISPs. RIP V1 and V2 are also IGPs.

Routers on the edge of the AS generate special LSAs (AS-External-LSAs) for the rest of the AS. There is also an address-forwarding mechanism that allows an OSPF router to obtain a route from a specified location. This feature allows a customer to introduce static routes for their network from a central router.

Autonomous Systems can be large. It is not necessary for the whole AS to know everything about all routes. Each AS might be broken down into areas. All routing information must be identical within an area. Routing between areas goes through a *backbone*. All routers on a backbone have to be able to communicate with each other. Since they belong to the same area (area 0 of a particular AS), they also all have to agree. *Area Border Routers* (ABRs) have one interface defined to run in the backbone area. Other interfaces can then be defined to run in a different area.

The following figure is a sample configuration of OSPF areas. It shows a large internal network and backbone terminating at a router.



For additional documentation on OSPF processing, see the official Quagga web site at <http://www.nongnu.org/quagga/docs.html>.



Tip: You should use OSPF only if you have identified that your routing topology is too complicated to use only static routing or the Routing Information Protocol (RIP). OSPF is a complex IP routing protocol and deploying OSPF should involve discussions between routing subject matter experts and security subject matter experts.

To implement OSPF processing on the Sidewinder, you must create an enabled rule with OSPF Routing Server selected in the Applications field and the Source and Destination Zones set to Any. You can control which routers the OSPF Routing Server can communicate with by managing the source and destination endpoints in the OSPF Routing Server rule. Each zone will have no more than a single OSPF Routing Server instance to handle the network traffic for all interfaces assigned to the zone.

The Sidewinder currently runs version 0.99.21 of the OSPF Routing Server. This is the most stable version of the OSPF Routing Server available from Quagga. The OSPF implementation on the Sidewinder supports all of the standards specified in RFC 2328.

Configuring OSPF

These are the high level steps to set up OSPF on Sidewinder.

- 1) Sketch a diagram showing your planned Sidewinder configuration (similar to the diagrams in *What does RIP do*). Include the following items on your diagram:
 - configuration of the routers to which the firewall connects
 - OSPF areas in the network(s)
 - the Sidewinder interfaces (zones)
- 2) Define one or more netgroups for the routers to which the firewall connects.
- 3) Configure one or more rules for the OSPF traffic.
- 4) Configure the appropriate OSPF parameters.

Using OSPF in your network is a two-step process: First you must create a rule that allows OSPF Routing Server traffic. Then you must configure the OSPF Routing Server with the appropriate network information and processing options.

Related concepts

[OSPF processing options](#) on page 433

[What RIP does](#) on page 420

Related tasks

[Create a rule for the OSPF Routing Server](#) on page 431

[Manage network objects](#) on page 86

Create a rule for the OSPF Routing Server

Enable access to the OSPF Routing Server configuration file.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the new rule.
- 4) In the **Applications** field, select **OSPF Routing Server**.
- 5) Set both the **Source Zone** and the **Destination Zone** fields to **Any**.
- 6) Configure the other **Source** and **Destination** fields as necessary to enforce your OSPF security policy.

7) Save your changes.

For the firewall to pass OSPF traffic, you now need to configure the OSPF Routing Server configuration file with the settings appropriate for your security policy. See the following section for the preferred method for enabling and disabling the OSPF Routing Server.

Configure basic OSPF Routing Server processing

There are several ways to configure the OSPF Routing Server on the Sidewinder.

- Telneting into the OSPF Routing Server on the firewall and using a command line interface.
- Using the Admin Console File Editor to edit the OSPF Routing Server configuration file.
- Using a different file editor, such as vi, to edit the OSPF Routing Server configuration file.

Because the command line method provides OSPF Routing Server help and validates commands as they are entered, the following sections focus on this method. The same commands and functionality described here are valid when using the other methods, but require different formatting. Be sure that you are familiar with the OSPF Routing Server formatting conventions before using those methods.

For additional documentation on OSPF processing, see the official Quagga web site at <http://www.nongnu.org/quagga/docs.html>.

Steps

- 1) Using a command line session, log on to the firewall and switch to the Admn domain by entering:

```
srole
```

- 2) Telnet into the Sidewinder OSPF Routing Server by entering:

```
telnet localhost ospfd
```

A password prompt appears.

- 3) Enter zebra.

A `ospfd>` prompt appears.

- 4) Enable the full command set by entering:

```
ospfd>en
```

The prompt changes to `ospfd#` to indicate that the full command set is enabled.

- 5) Enable configuration mode by entering:

```
(config)#conf t
```

The prompt changes to `ospfd(config)#` to indicate that configuration mode is enabled.

- 6) Enable the OSPF Routing Server and configure it to advertise routes, receive updates, and install routes in the local routing table by entering the following commands:
- ```
(config)#router ospf
(config-router)#network X.X.X.X/mask area n.n.n.n
```
- where
- X.X.X.X/mask* is the subnet and network mask of the interface on which you are enabling OSPF. You can enter multiple network statements.
- n.n.n.n* is the area within the AS, such as 0.0.0.0 for the backbone area.
- 7) [Optional] To make changes persistent across restarts, write the changes to the configuration file by entering:
- ```
(config)#write
```

Result

The OSPF Routing Server is now enabled and is advertising, receiving, and creating routing information. See the following section for information on other configuration options.

To disable the OSPF Routing Server, follow *Step 1* through *Step 5* in the previous procedure, and then enter:

```
(config)#no router ospf
```

The OSPF Routing Server is now disabled and will not participate in routing.

OSPF processing options

As with RIP, only administrators who are experienced with routing in general, and OSPF dynamic routing in particular, should configure the OSPF Routing Server.

These commands are presented as they are entered at a command line interface. They also assume that you have entered the appropriate network and area statements when you first accessed the OSPF Routing Server. Another option is to configure these options by using the Admin Console File Editor or other file editor to edit the configuration file directly. If you chose to modify the file directly, pay close attention to formatting. See the Quagga documentation at <http://www.nongnu.org/quagga/docs.html> for formatting assistance.



Tip: Use the OSPF Routing Server online help, available when using the CLI, for details on modifying the commands given here as well as other supported configurations. To access the OSPF Routing Server online help, enter a mode (such as `router ospf` or `route-map`) and then enter `?` or `list`. You must be currently running a mode to see its documentation.

In general, the OSPF configuration options are similar to the RIP configuration options, particularly the `route-map`, `prefix-list`, and `redistribution` commands. However, the servers' implementation differences of the `passive-interface` command is worth noting.

For both servers, the `passive-interface` command enables the routing protocol on all interfaces that are on the specified subnet. For RIP, the server receives updates and creates routes in the local routing table, but does not advertise routes. For the OSPF Routing Server, the server passively advertises the local interface information, but does not form adjacency with other routers over the specified interface.

For OSPF, use these commands to configure this option:

```
(config)#router ospf
(config-router)#passive-interface if_name
```

where *if_name* is the interface name of the zone that is to learn routes, but does not send HELLOs to other routers. Use `default` to set this configuration on all interfaces.

Related concepts[RIP processing options](#) on page 425

Viewing and comparing OSPF configurations

The Admin Console provides tools to help you manage your OSPF configuration.

You can use these tools to quickly view the entire configuration file, compare different states of the configuration file, or list items such as the OSPF neighbours and routes. You can also use the OSPF area to edit the configuration file using the File Editor and to overwrite the configuration to be used the next time the OSPF Routing Server restarts.

To use these tools, select **Network > Routing > Dynamic Routing > OSPF**.

On this window, you can do the following:

- **Edit a configuration file** — Click **Edit** to open the configuration file using the Admin Console File Editor. Edit the file as needed and then save your changes. The firewall automatically restarts the OSPF Routing Server.



Note: Remember to create a rule using the OSPF Routing Server before attempting to pass OSPF traffic.

- **View and compare files** — Select an option from the list and then click **Retrieve**. A pop-up window appears displaying the requested information. Close this pop-up to return to the main OSPF window.
- **Save the running configuration to the configuration file** — Click **Overwrite** to save the running configuration. The running configuration and the starting configuration are now the same.

Related tasks[Create a rule for the OSPF Routing Server](#) on page 431[Configure basic OSPF Routing Server processing](#) on page 432

Concepts of OSPF IPv6

The OSPF IPv6 protocol concepts are the same as OSPF for IPv4, with the following differences.

- OSPF IPv6 processing is performed by the Sidewinder OSPF IPv6 Routing Server.
- New LSAs have been created to carry IPv6 addresses and prefixes.
- OSPF IPv6 multicasts using the following broadcast addresses:
 - **AllSPFRouters** — This multicast address has been assigned the value FF02::5. All routers running OSPF should be prepared to receive packets sent to this address. Hello packets are always sent to this destination.
 - **AllIDRouters** — This multicast address has been assigned the value FF02::6. Both the Designated Router and Backup Designated Router must be prepared to receive packets destined to this address.

See RFC 2740 for more information.

Create a rule for the OSPF IPv6 Routing Server

Enable access to the OSPF IPv6 Routing Server configuration file.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the rule.
- 4) In the **Applications** field, select **OSPF IPv6 Routing Server**.
- 5) Set both the **Source Zone** and the **Destination Zone** fields to **Any**.
- 6) Configure the other **Source** and **Destination** fields as necessary to enforce your OSPF IPv6 security policy.
- 7) Save your changes.

Configure basic OSPF IPv6 Routing Server processing

There are several ways to configure the OSPF IPv6 Routing Server on the Sidewinder.

- Telneting into the OSPF IPv6 Routing Server on the firewall and using a command line interface.
- Using the Admin Console File Editor to edit the OSPF IPv6 Routing Server configuration file.
- Using a different file editor, such as vi, to edit the OSPF IPv6 Routing Server configuration file.

Because the command line method provides OSPF Routing Server help and validates commands as they are entered, the following sections focus on this method. The same commands and functionality described here are valid when using the other methods, but require different formatting. Be sure that you are familiar with OSPF IPv6 Routing Server formatting conventions before using those methods.

For additional documentation on OSPF IPv6 processing, see the official Quagga web site at <http://www.nongnu.org/quagga/docs.html>.

Steps

- 1) Using a command line session, log on to the firewall and switch to the Admn domain by entering:

```
srole
```
- 2) Telnet into the Sidewinder OSPF IPv6 Routing Server by entering:

```
telnet localhost ospf6d
```

A password prompt appears.

- 3) Enter `zebra`.
An `ospf6d>` prompt appears.
- 4) Enable the full command set by entering:
`ospf6d>en`
The prompt changes to `ospf6d#` to indicate that the full command set is enabled.
- 5) Enable configuration mode by entering:
`(config)#conf t`
The prompt changes to `ospf6d(config)#` to indicate that configuration mode is enabled.
- 6) Enable the OSPF IPv6 Routing Server and configure it to advertise routes, receive updates, and install routes in the local routing table by entering the following commands: -
`(config)#router ospf6`
`(config-router)router-id X.X.X.X`
`(config-router)#interface XXX area n.n.n.n`
where
 - `X.X.X.X` is the value other routers will know this router by. Router IDs are the IPv4 size of 32-bits.
 - `XXX` is the interface NIC on which you are enabling OSPF IPv6. You can enter multiple interfaces.
 - `n.n.n.n` is the area within the AS, such as 0.0.0.0 for the backbone area.
- 7) [Optional] To make changes persistent across restarts, write the changes to the configuration file by entering:
`(config)#write`

Result

The OSPF IPv6 Routing Server is now enabled and is advertising, receiving, and creating routing information. To disable the OSPF IPv6 Routing Server, follow *Step 1* through *Step 5* in the previous procedure, and then enter:

```
(config)#no router ospf6
```

The OSPF IPv6 Routing Server is now disabled and will not participate in routing.

Viewing and comparing OSPF IPv6 configurations

The Admin Console provides tools to help you manage your OSPF IPv6 configuration.

You can use these tools to quickly view the entire configuration file, compare different states of the configuration file, or list items such as the OSPF IPv6 neighbors and routes. You can also use the OSPF IPv6 area to edit the configuration file using the File Editor and to overwrite the configuration to be used the next time the OSPF IPv6 Routing Server restarts.

To use these tools, select **Network > Routing > Dynamic Routing > OSPFIPv6**. The **OSPF IPv6** window appears.

On this window, you can do the following:

- **Edit a configuration file** — Click **Edit** to open the configuration file using the Admin Console File Editor. Edit the file as needed and then save your changes. The firewall automatically restarts the OSPF IPv6 Routing Server.



Note: Remember to create a rule using the OSPF IPv6 Routing Server before attempting to pass OSPF IPv6 traffic.

- **View and compare files** — Select an option from the list and then click **Retrieve**. A pop-up window appears displaying the requested information. Close this pop-up to return to the main **OSPF IPv6** window.
- **Save the running configuration to the configuration file** — Click **Overwrite** to save the running configuration. The running configuration and the starting configuration are now the same.

What BGP passes

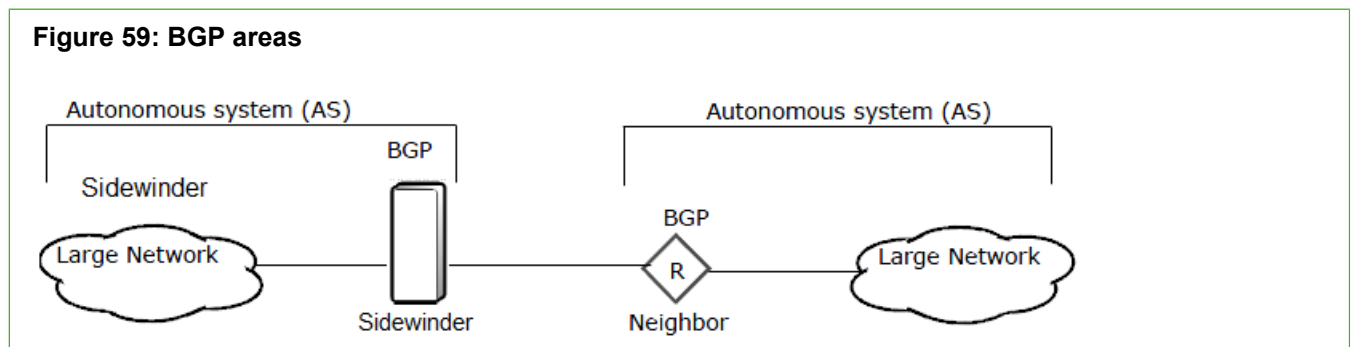
The Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) used to pass routing information between Autonomous Systems (AS).

Unlike OSPF, which is an Interior Gateway Protocol (IGP), BGP is used to connect to external routers, such as your ISP. It does, however, learn information from an interior network that it then passes to an external network.



Note: IPv4 and IPv6 are supported for BGP on Sidewinder.

Routers using BGP are commonly located at the perimeter of an AS, as shown in the following figure.



Routers employing BGP use TCP connections to communicate with peer routers, known as neighbors. After a connection is established, routing information is exchanged. Traffic is passed on port 179. The connection is maintained using keep-alives that are sent by both neighbors at a default rate of every 60 seconds, with a 3 minute timeout.

On the Sidewinder, BGP processing is performed by the Sidewinder BGP Routing Server. To implement BGP processing, the BGP Routing Server must be configured and there must be an active rule that allows BGP broadcasts. You can control which routers the BGP Routing Server can communicate with by managing the source and destination endpoints in the BGP Routing Server access control rule. Each zone will have no more than a single BGP Routing Server instance to handle the network traffic for all interfaces assigned to the zone.

As with the other Sidewinder dynamic routing protocols, see the Quagga documentation for a list of supported features.

IPv4 and IPv6 support for BGP

BGP peers can exchange both IPv4 and IPv6 routes.

These configurations are supported:

- **BGP IPv4** — BGP IPv4 route distribution over IPv4 or IPv6 network transport
- **BGP IPv6** — BGP IPv6 route distribution over IPv6 or IPv4 network transport

Configuring BGP

These are the high level steps to set up BGP on Sidewinder.

- 1) Sketch a diagram showing your planned Sidewinder configuration (similar to the diagrams in *BGP areas*). Include the following items on your diagram:
 - configuration of the routers to which the firewall connects
 - BGP areas in the network(s)
 - the Sidewinder interfaces (zones)
- 2) Define one or more netgroups for the routers to which the firewall connects.
- 3) Configure one or more rules for the BGP traffic.
- 4) Configure the appropriate BGP parameters.

Using BGP in your network is a two-step process: First you must create a rule that allows BGP Routing Server traffic. Then you must configure the BGP Routing Server with the appropriate network information and processing options.

Related concepts

[BGP processing options](#) on page 440

Related tasks

[Create a rule for the BGP Routing Server](#) on page 438

[Manage network objects](#) on page 86

Create a rule for the BGP Routing Server

Enable access to the BGP Routing Server configuration file.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the new rule.
- 4) In the **Applications** field, select **BGP Routing Server**.
- 5) Set both the **Source Zone** and the **Destination Zone** fields to **Any**.
- 6) Configure the other **Source** and **Destination** fields as necessary to enforce your BGP security policy.
- 7) Save your changes.

Result

For the firewall to pass BGP traffic, you now need to configure the BGP Routing Server configuration file with the settings appropriate for your security policy. See the following section for the preferred method for enabling and disabling the BGP Routing Server server.

Configure basic BGP Routing Server processing

There are several ways to configure the BGP Routing Server on the Sidewinder.

- Telneting into the BGP Routing Server server on the firewall and using a command line interface.
- Using the Admin Console File Editor to edit the BGP Routing Server configuration file.
- Using a different file editor, such as vi, to edit the BGP Routing Server configuration file.

Because the command line method provides BGP Routing Server help and validates commands as they are entered, the following sections focus on this method. The same commands and functionality described here are valid when using the other methods, but require different formatting. Be sure that you are familiar with BGP Routing Server formatting conventions before using those methods.

For additional documentation on BGP processing, see the official Quagga web site at <http://www.nongnu.org/quagga/docs.html>.

Steps

- 1) Using a command line session, log on to the firewall and switch to the Admn domain by entering:

```
role
```
- 2) Telnet into the Sidewinder BGP Routing Server by entering:

```
telnet localhost bgpd
```

A password prompt appears.
- 3) Enter `zebra`.
A `bgpd>` prompt appears.
- 4) Enable the full command set by entering:

```
bgpd>en
```

The prompt changes to `bgpd#` to indicate that the full command set is enabled.

- 5) Enable configuration mode by entering:

```
(config)#conf t
```

The prompt changes to `bgpd(config)#` to indicate that configuration mode is enabled.

- 6) Enable the BGP Routing Server and configure it to advertise routes, receive updates, and install routes in the local routing table by entering the following commands:

```
(config)#router bgp
```

```
(config-router)#network X.X.X.X/mask
```

where `X.X.X.X/mask` is the subnet and network mask of the interface on which you are enabling BGP. You can enter multiple network statements.

- 7) [Optional] To make changes persistent across restarts, write the changes to the configuration file by entering:

```
(config)#write
```

Result

The BGP Routing Server is now enabled and is advertising, receiving, and creating routing information. See the following section for information on other configuration options.

To disable the BGP Routing Server, follow Step 1 through Step 5 in the previous procedure, and then enter:

```
(config)#no router bgp
```

The BGP Routing Server is now disabled and will not participate in routing.

BGP processing options

As with RIP and OSPF, only administrators who are experienced with routing in general, and BGP dynamic routing in particular, should configure the BGP Routing Server.

These commands are presented as they are entered at a command line interface. They also assume that you have entered the appropriate network and area statements when you first accessed the BGP Routing Server. Another option is to configure these options by using the Admin Console File Editor or other file editor to edit the configuration file directly. If you chose to modify the file directly, pay close attention to formatting. See the Quagga documentation at <http://www.nongnu.org/quagga/docs.html> for formatting assistance.



Tip: Use the BGP Routing Server online help, available when using the command line interface, for details on modifying the commands given here as well as other supported configurations. To access the BGP Routing Server online help, enter a mode (such as `router bgp` or `route-map`) and then enter `?` or `list`. You must be currently running a mode to see its documentation.

In general, the BGP configuration options are similar to the RIP and OSPF configuration options, particularly the `route-map`, `prefix-list`, and `redistribution` commands. However, instead of using interface names to identify the source and destination of routing information, BGP uses names of neighbors.

Related concepts

[RIP processing options](#) on page 425

Configure BGP authentication

To further secure network borders, enable BGP authentication through a two-step process.

BGP uses the TCP MD5 authentication option to authenticate BGP neighbors. Enable BGP authentication, then create a new IPsec VPN definition for BGP neighbors that require authentication.

Enable BGP authentication

Use the BGP command line utility to enable TCP MD5 authentication for BGP neighbors.

Steps

- 1) From the command line, log on and enter `sr0le` to switch to the Admn domain.

- 2) Telnet into the Sidewinder BGP routing server by entering:

```
telnet localhost bgpd
```

- 3) When prompted for a password, enter `zebra`.

- 4) At the `bgpd>` command prompt, enter `en`.

The command prompt changes to `bgpd#` to indicate that the full command set is enabled.

- 5) Enable configuration mode by entering:

```
conf t
```

The command prompt changes to `bgpd(config)#` to indicate that configuration mode is enabled.

- 6) Enter the BGP router configuration area for the Autonomous System (AS) to enable neighbor-specific options:

```
router bgp <AS Number>
```

where `<AS Number>` is the specific local Autonomous System number. The command prompt changes to `bgpd(config-router)#`.

- 7) Enable the authentication option for each routing neighbor requiring authentication:

```
neighbor 10.10.10.10 password password
```

where `10.10.10.10` is the neighbor address, either an IPv4 or IPv6 address.



Note: The authentication password provided to the BGP routing server through the BGP command line (or config file) does not set the authentication key. It is used only as an indication that the specified neighbor must use authentication. See *Create an IPsec VPN definition* for management of the authentication password.


- 8) To make it permanent, write the changes to the configuration file by entering:

```
write
```


Related tasks[Create an IPsec VPN definition](#) on page 442

Create an IPsec VPN definition

Each BGP neighbor requiring authentication must have a separate IPsec VPN definition.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Network > VPN Configuration > VPN Definitions**, then click **New**.
- 2) On the **General** tab, enter these details.
 - **Name** — Specify an appropriate name for the new VPN definition to a BGP neighbor.
 - **Mode** — Select **Manually Keyed VPN**.
 - **Zone** — Select the zone associated with the BGP neighbor.
 - **Encapsulation** — Select **Transport**.
 - **IP Version** — Select either IPv4 or IPv6, based on the BGP neighbor address family.
 - **Remote IP** — Specify the address of the BGP neighbor for which MD5 authentication has been enabled in the BGP agent configuration.
- 3) On the **Crypto** tab, enter these details.
 - **IPsec Transformations** — Select **Authentication Header (AH)**.
 - **Authentication Hash** — Select **tcp-md5**.
 - **AH Inbound Key** — Specify the key or password string to use for authentication.
 - **AH Outbound Key** — Specify the key or password string to use for authentication.



Note: Most router implementations use a single password string for authentication keys for both inbound and outbound processing. To interoperate with such hosts, the inbound and outbound keys are set to the same password value, matching the configuration of the remote routing neighbor.
- 4) Leave all other values as default.
- 5) Click **Add** to save the new VPN definition.
- 6) Save your changes.

Viewing and comparing BGP configurations

The Admin Console provides tools to help you manage your BGP configuration.

You can use these tools to quickly view the entire configuration file, compare different states of the configuration file, or list items such as the BGP neighbours and routes. You can also use the BGP area to edit the configuration

file using the File Editor and to manually overwrite the configuration to be used the next time the BGP Routing Server restarts.

To use these tools, select **Network > Routing > Dynamic Routing > BGP**.

On this window, you can do the following:

- **Edit a configuration file** — Click **Edit** to open the configuration file using the Admin Console File Editor. Edit the file as needed and then save your changes. The firewall automatically restarts the BGP Routing Server.



Note: Remember to create a rule using the BGP Routing Server before attempting to pass BGP traffic.

- **View and compare files** — Select an option from the list and then click **Retrieve**. A pop-up window appears displaying the requested information. Close this pop-up to return to the main BGP window.
- **Save the running configuration to the configuration file** — Click **Overwrite** to save the running configuration. The running configuration and the starting configuration are now the same.

Related concepts

[Configuring BGP](#) on page 438

Related tasks

[Create a rule for the BGP Routing Server](#) on page 438

Why the PIM-SM protocol is used

The Protocol Independent Multicast - Sparse Mode (PIM-SM) protocol is used to route traffic to multicast groups.



Note: IPv6 is not supported for PIM-SM on Sidewinder.

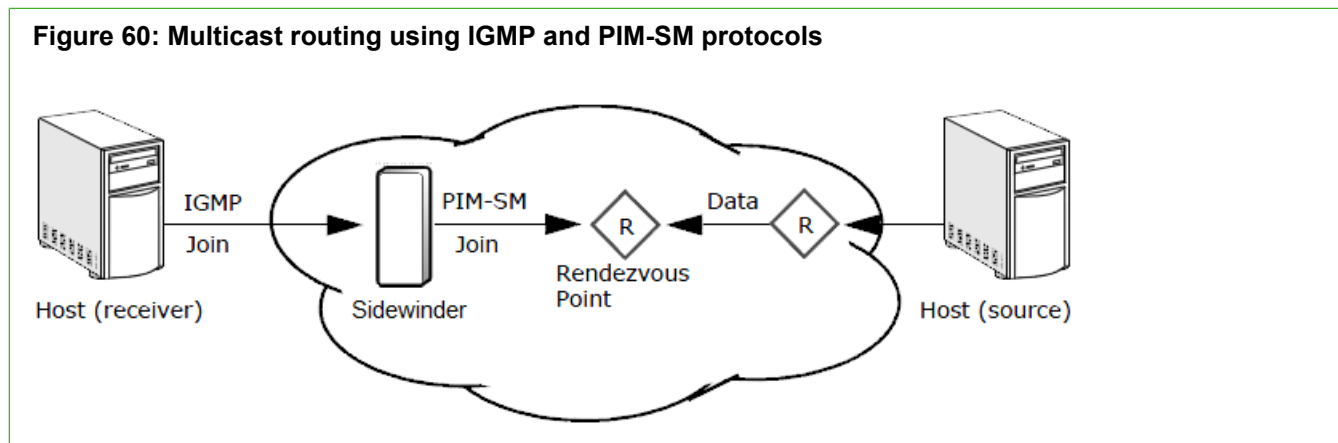
Multicast is communication between a single or multiple senders and multiple receivers on a network. The Sidewinder uses a XORP routing package which contains IGMP and PIM-SM protocols to route multicast traffic:

- The Internet Group Management Protocol (IGMP) is used by hosts and adjacent routers to establish multicast group memberships. IGMP tells routers that a host wants to receive multicast traffic for the specified multicast group.
- The PIM-SM protocol sets up a multicast forwarding table in routers. Multicast traffic is directed to a rendezvous point (RP), which distributes it toward PIM-registered receivers.

When a host wants to join a multicast session, IGMP sends a join request to its gateway router for a multicast group. Since the gateway router doesn't have information about the source address, it will send a PIM join back to the rendezvous point, which will contain the source information.

The rendezvous point facilitates the route setup between the sender and receiver. The sending gateway router sends multicast data to a rendezvous point encapsulated in a unicast PIM packet.

Once a gateway router with direct connection to the receiver's network has received traffic from the source, the gateway router might start a process to build a direct path from the sender to the source.

Figure 60: Multicast routing using IGMP and PIM-SM protocols

Configure PIM-SM (XORP PIMD)

To configure a Sidewinder to route multicast traffic using PIM-SM, you must perform the following high-level procedures.



Important: XORP uses the lowest IP address found in the interface table. The XORP process stores the IP addresses in ascending order. While creating an HA pair, if the individual interface IP address (for example, 10.10.10.2) is lower than the cluster IP address (for example, 10.10.10.3), then PIM_HELLO messages are sent with the source IP address of the individual IP address. Review the XORP shell `show pim interface` command output to verify. If an interface is configured for XORP with multiple IP addresses, always designate the lowest IP address for XORP peer communication.

- 1) Create policy rules to enable XORP PIMD and allow multicast traffic and PIM traffic forwarding.
- 2) Configure XORP PIMD.
- 3) Configure IGMP.
- 4) Configure PIM-SM.
- 5) Restart XORP PIMD.

It is recommended that you make all of these configuration changes at one time, since you must restart XORP PIMD to initialize your changes.



Note: When making subsequent changes to PIM-SM, there are two types of changes that require different procedures.

Related reference

[Exceptions to making PIM-SM changes on page 454](#)

Create policy rules

You must create the policy rules to allow PIM-SM multicast routing.

Create a rule to enable the XORP PIMD server

Enable the XORP PIMD server.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the new rule.
- 4) From the **Applications** list, select **XORPPIMD**.
- 5) Set both the **Source Zone** and the **Destination Zone** fields to **Any**.
- 6) Configure the other **Source** and **Destination** fields as necessary to enforce your PIM-SM security policy.
- 7) Save your changes.

Create a rule to enable PIM traffic forwarding to rendezvous points and bootstrap routers

Create a rule to allow PIM-SM traffic forwarding.

Steps

- 1) Select **Policy > Access Control Rules**
- 2) Click **New**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the new rule.
- 4) From the **Applications** list, select **PIM**.
- 5) Set both the **Source Zone** and the **Destination Zone** fields to **Any**.
- 6) Configure the other **Source** and **Destination** fields as necessary to enforce your PIM-SM security policy. Include all rendezvous points and bootstrap routers within the PIM network.
- 7) Click **OK** and save your changes.

Create a rule to enable multicast traffic

Create a rule to allow multicast traffic.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Click **New**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Type a name for the new rule.
- 4) From the **Applications** list, select **TCP/UDP**.
- 5) In the **UDP ports** field, select the UDP ports your multicast applications will be using.
- 6) Configure the **Source** and **Destination** fields as necessary to enforce your multicast security policy. Include the multicast groups in the **Destination Endpoint** field.
- 7) Click **OK** and save your changes.

Configure XORP PIMD

Make the necessary configurations to the XORP PIMD configuration file.

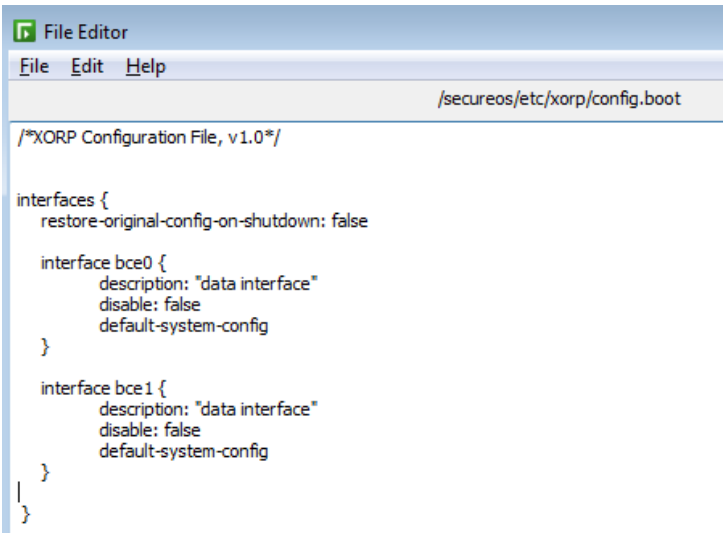
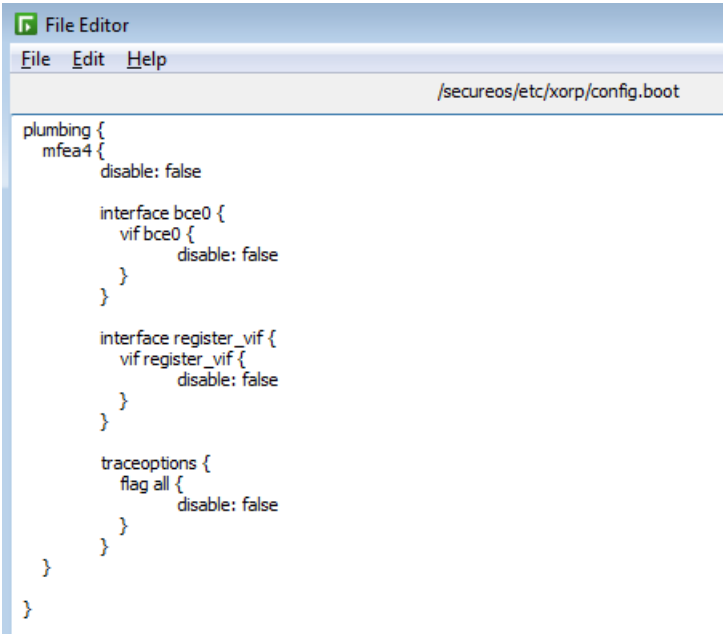
Steps

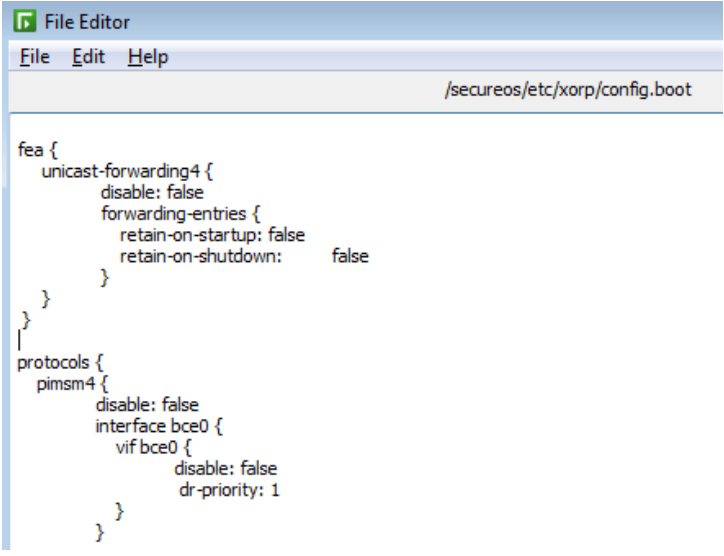
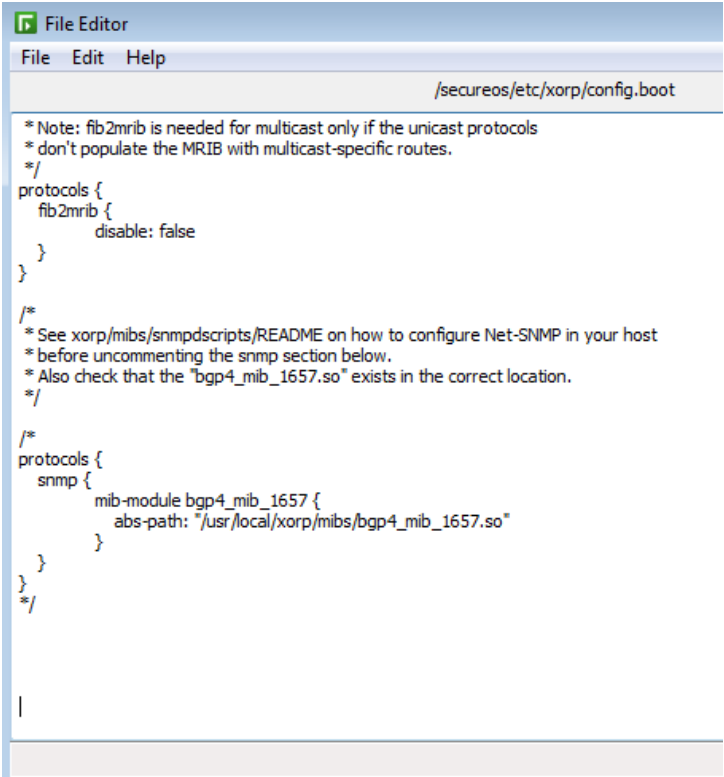
- 1) Select **Network > Routing > Dynamic Routing > PIMSM**.
- 2) Click **Edit**. The XORP PIMD configuration file opens in the File Editor.



Tip: For option descriptions, click **Help**.

- 3) Verify that the interface names in the file are correct.
- 4) Remove the comments for these parameters:

Parameters	PIM-SM Editor window
<p>Interfaces you want to run multicast over. <i>default-system-config</i> causes XORP PIMD to use the interface configuration from the system kernel.</p>	 <pre> /*XORP Configuration File, v1.0*/ interfaces { restore-original-config-on-shutdown: false interface bce0 { description: "data interface" disable: false default-system-config } interface bce1 { description: "data interface" disable: false default-system-config } } </pre>
<p><i>mfea4</i> identifies which interfaces are being used for multicast traffic. <i>register_vif</i> is necessary for XORP processing.</p>	 <pre> plumbing { mfea4 { disable: false interface bce0 { vif bce0 { disable: false } } interface register_vif { vif register_vif { disable: false } } traceoptions { flag all { disable: false } } } } </pre>

Parameters	PIM-SM Editor window
<p><i>fea</i> tells XORP PIMD how to locate unicast routes.</p>	 <pre> File Editor File Edit Help /secureos/etc/xorp/config.boot fea { unicast-forwarding4 { disable: false forwarding-entries { retain-on-startup: false retain-on-shutdown: false } } } protocols { pimsm4 { disable: false interface bce0 { vif bce0 { disable: false dr-priority: 1 } } } } </pre>
<p><i>fib2mrib</i> tells PIM-SM to use the unicast routing table to find a route to the rendezvous points and to the sender.</p>	 <pre> File Editor File Edit Help /secureos/etc/xorp/config.boot * Note: fib2mrib is needed for multicast only if the unicast protocols * don't populate the MRIB with multicast-specific routes. */ protocols { fib2mrib { disable: false } } /* * See xorp/mibs/snmpdscrips/README on how to configure Net-SNMP in your host * before uncommenting the snmp section below. * Also check that the "bgp4_mib_1657.so" exists in the correct location. */ /* protocols { snmp { mib-module bgp4_mib_1657 { abs-path: "/usr/local/xorp/mibs/bgp4_mib_1657.so" } } } */ </pre>

Configure IGMP

Make the necessary modifications to the XORP PIMD configuration file.

Steps

- 1) [If necessary] Select **Network > Routing > Dynamic Routing > PIMSM** and click **Edit** to open the XORP PIMD configuration file.



Tip: For option descriptions, click **Help**.

- 2) Add an IGMP clause to the configuration file, specifying the interfaces to networks where hosts are receiving multicast packets. See the example below.

Figure 61: IGMP added to the XORP PIMD configuration file

```
File Editor
File Edit Help
/secureos/etc/xorp/config.boot

protocols {
    igmp {
        disable: false
        interface em3 {
            vif em3 {
                disable: false
            }
        }
    }
}

pimsm4 {
```



Note: To disable IGMP for the network, disable the corresponding interface in the igmp section.

- 3) Save your changes.

Configure PIM-SM

You need to perform two tasks for a dynamic PIM-SM configuration.

Specify interfaces

Specify the interfaces that will run PIM-SM.

Steps

- 1) [If necessary] Select **Network > Routing > Dynamic Routing > PIMSM** and click **Edit** to open the XORP PIMD configuration file.



Tip: For option descriptions, click **Help**.

- 2) Configure the interfaces that will run PIM-SM.
 - For each interface, an interface statement within the *pimsm4* section of the config file must be included.
 - *register_vif* must be included.

Figure 62: Bootstrap router parameters

```

File Editor
File Edit Help
/secureos/etc/xorp/config.boot

pimsm4 {
  disable: false
  interface bce0 {
    vif bce0 {
      disable: false
      dr-priority: 1
    }
  }

  interface bce1 {
    vif bce1 {
      disable: false
      dr-priority: 1
    }
  }

  interface register_vif {
    vif register_vif {
      disable: false
    }
  }
}

```

Configure the rendezvous points

There are two ways to configure the rendezvous point: dynamically with a bootstrap router or using static configuration.

The bootstrap (dynamic) protocol is useful for large networks.

- You can have multiple rendezvous points—if one rendezvous point goes away, another one is elected.
- You can specify whether you want to be a rendezvous point, and you can specify whether you want to communicate with another router that is a rendezvous point.

- You do not have to configure rendezvous points—rendezvous points are learned. You can specify which interfaces on your firewall can learn the rendezvous points.

Static PIM-SM is a simpler configuration that is useful for smaller networks, for example, if you have only two PIM routers or if your ISP provides the rendezvous point.

To configure rendezvous points dynamically with a bootstrap router:

Steps

- 1) [If necessary] Select **Network > Routing > Dynamic Routing > PIMSM** and click **Edit** to open the XORP PIMD configuration file.



Tip: For option descriptions, click **Help**.



Note: You cannot change the `bsr-priority` (bootstrap router priority) setting in this file. If you need to change this setting, see *Change the bsr-priority setting* for instructions.

Figure 63: Bootstrap router parameters

```

File Editor
File Edit Help
/secureos/etc/xorp/config.boot

bootstrap {
  disable: false
  cand-bsr {
    scope-zone 224.0.0.0/4 {
      cand-bsr-by-vif-name: "bce0"
    }
  }

  cand-rp {
    group-prefix 224.0.0.0/4 {
      cand-rp-by-vif-name: "bce0"
    }
  }
}

switch-to-spt-threshold {
  /* approx. 1K bytes/s (10Kbps) threshold */
  disable: false
  interval: 100
  bytes: 102400
}

traceoptions {
  flag all {
    disable: false
  }
}
}

```

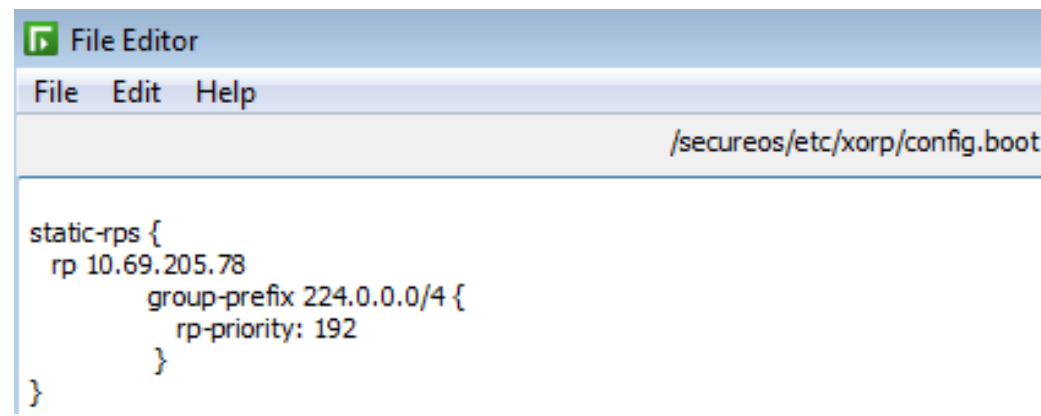
- 2) Remove the comments from the bootstrap router and rendezvous points.
 - *cand-bsr* is the bootstrap protocol that selects a bootstrap router. The bootstrap router tells all PIM-SM routers what the rendezvous points are.
 - *cand-rp* tells the bootstrap router that this router is a candidate to be a rendezvous point.
 - *switch-to-spt-threshold* lets you specify the data rate at which the router selects the shortest path between the sender and the receiver.
 - If you have a lot of multicast traffic and use multicast for a long time, finding a shortest path is useful.
 - If you don't have much traffic, or if you use multicast for a short time, finding a shortest path isn't necessary.
 - *traceoptions* sends debug tracing to syslog.

- 3) Save your changes.

To configure rendezvous points using static configuration:

- 1) [If necessary] Select **Network > Routing > Dynamic Routing > PIMSM** and click **Edit** to open the XORP PIMD configuration file.
- 2) Add *static-rps* clause to the configuration file, specifying the rendezvous point for a range of group prefixes. See the example below.
 - If more than one rendezvous point is specified for a group, the rendezvous point with the lowest priority is used.
 - All PIM-SM routers must be configured with the same rendezvous points.

Figure 64: Bootstrap router parameters



```

File Editor
File Edit Help
/secureos/etc/xorp/config.boot

static-rps {
  rp 10.69.205.78
    group-prefix 224.0.0.0/4 {
      rp-priority: 192
    }
}

```

Related tasks

[Change the bsr-priority setting on page 455](#)

Restart XORP PIMD

Restart the XORP PIMD server.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Select the rule that uses XORP PIMD and click **Modify**.



Tip: For option descriptions, click **Help**.

- 3) Clear the **Enable** box.
- 4) Click **OK** and save your changes.
- 5) Select the rule that uses the XORP PIMD and click **Modify**.
- 6) Select the **Enable** box.
- 7) Click **OK** and save your changes.

Exceptions to making PIM-SM changes

The procedures in this section explain how to configure XORP PIMD using the Sidewinder Admin Console. To configure XORP PIMD through a command line interface, you use the XORP PIMD command shell *xorpsh*

The Admin Console PIM-SM window, *xorpsh*, and any file editor opens the same `config.boot` file (`/secureos/etc/xorp/config.boot`). However, the PIM-SM editor and *xorpsh* interact, which can cause conflicts.

To avoid conflicts, there are two types of changes to PIM-SM that require different procedures:

- Disabling and enabling PIM-SM
- Changing the `bsr-priority` setting

Disable and enable XORP PIMD

You cannot use *xorpsh* to enable or disable PIM-SM. To avoid an error message, you must enable or disable the rule that uses XORP PIMD.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Select the rule that uses XORPPIMD and click **Modify**.



Tip: For option descriptions, click **Help**.

- 3) Make the appropriate action:
 - a) To disable XORP PIMD, clear the **Enable** box.

- b) To enable XORP PIMD, select the **Enable** box.
- 4) Click **OK** and save your changes.

Change the bsr-priority setting

The procedures in this section explain how to configure XORP PIMD using the Sidewinder Admin Console. To configure XORP PIMD through a command line interface, you use the XORP command shell *xorpsh*.


The Admin Console's **PIMSM** window, *xorpsh*, and any file editor open the same `config.boot` file (`/secureos/etc/xorp/config.boot`). However, the PIMSM editor and *xorpsh* interact, which can cause conflicts.

To avoid conflicts, you cannot change the bsr-priority (bootstrap) parameter using the Edit function on the **PIMSM** window. To avoid an error message, you must stop XORP PIMD, change the parameter, and restart the XORP server.

To change the bsr-priority parameter:

Steps

- 1) Stop XORP PIMD:
 - a) Select **Policy > Access Control Rules**.
 - b) Select the rule that uses XORP PIMD and click **Modify**.

 **Tip:** For option descriptions, click **Help**.
 - c) Clear the **Enable** box.
 - d) Click **OK** and save your changes.
- 2) Change the bsr-priority parameter:
 - a) Select **Maintenance > File Editor** and open the following firewall file:
`/secureos/etc/xorp/config.boot`
 - b) Make the desired change to the bsr-priority parameter.
 - c) Save your changes and close the File Editor.
- 3) Start XORP PIMD:
 - a) Select **Policy > Access Control Rules**.
 - b) Select the rule that uses XORP PIMD and click **Modify**.
 - c) Select the **Enable** box.
 - d) Click **OK** and save your changes.

Viewing XORP PIMD configurations

Use the **PIM-SM** window to view and configure PIM-SM routing parameters.

Select **Network > Routing > Dynamic Routing > PIMSM**. The **PIMSM** window appears.

On this window, you can do the following:

- **Edit a configuration file** — Click **Edit** to open the configuration file using the Admin Console File Editor. Edit the file as needed and then save your changes. The firewall automatically restarts XORP PIMD.
- **View and compare files** — Select an option from the list and then click **Retrieve**. A pop-up window appears displaying the requested information. Close this pop-up to return to the main **PIMSM** window.

Related tasks

[Configure PIM-SM \(XORP PIMD\)](#) on page 444

Dynamic routing in HA clusters

If you use dynamic routing in HA clusters, note the following considerations.

- [rip, ospf, and bgp] Add a router-id entry to the configuration file. You must specify an address, such as the cluster IP address.

For example, if 10.1.1.15 is your cluster IP address, configure the router-id like the following:

```
rip
router rip
network 10.1.1.15/32
ospf router ospf
router-id 10.1.1.15
network 10.1.1.15/32 area 0
bgp
router bgp
bgp router-id 10.1.1.15
```

In neighbor bgp routers:

```
router bgp
neighbor 10.1.1.15 remote-as 6665
```

- [ospf and rip] If you specify the networks or interfaces by IP address, use the cluster IP address.

Troubleshooting dynamic routing issues

If you need to troubleshoot dynamic routing issues, you can use the following commands to enable debugging, and then either display or save the log files.

- 1) Using a command line session, log on to the firewall and switch to the Admn domain by entering: `role`
- 2) Telnet into the appropriate dynamic routing server by entering one of the following command:
 - To access the OSPF Routing Server, enter:


```
telnet localhost ospfd
```
 - To access the BGP Routing Server, enter:


```
telnet localhost bgpd
```

- To access the RIP Routing Server, enter:

```
telnet localhost_n ripd
```

where *n* = the zone index of the zone used as the source zone in the enabled RIP Routing Server rule. Use `cf zone query` to look up a zone's index. It is also listed on the **Network > Zone Configuration** window as the ID.

A password prompt appears.

- 3) Enter `zebra`.

A `ripd>` prompt appears.



Note: The prompt will reflect the server you logged into.

- 4) Enable the full command set by entering:

```
ripd>en
```

The prompt changes to `ripd#` to indicate that the full command set is enabled.



Note: Enabling debugging at this prompt turns debugging on temporarily. To making debugging persistent, enter the `conf t` command before entering the debug commands.

- 5) Set the debug parameters by entering one or more commands similar to these examples:

```
ripd#debug protocol event
```

```
ripd#debug protocol packet [recv|send] [detail]
```

```
ripd#debug protocol zebra
```

where *protocol* is `rip` (case sensitive).

See the online help or Quagga documentation for `ospf` and `bgp` commands and for additional debugging flags.

- 6) View the log information in the current window by entering:

```
ripd#term monitor
```

To stop writing debug statement to the current window, enter:

```
ripd#term no monitor
```

- 7) [Optional] To save the log information to a log file, you can edit the configuration file directly and add this line:

```
log file filename
```

The default path for the log file is `/var/run/quagga`. To save the file in a different location, specify the entire path as part of the file name.

If you misconfigure your routing tables, you will need to disable the RIP Routing Server and make corrections to the tables and then restart the RIP Routing Server, either by writing the file changes or saving the configuration file using the Admin Console File Editor. Before restarting the RIP Routing Server, enter the following command at a UNIX prompt to flush the routing tables of all gateways:

```
route flush
```


DNS (domain name system)

Contents

- [Types of DNS modes](#) on page 459
- [Configuring transparent DNS](#) on page 460
- [Configuring firewall-hosted DNS](#) on page 461
- [Reconfiguring DNS](#) on page 477
- [DNS message logging](#) on page 480
- [Configuring DNSSEC](#) on page 480

The domain name system (DNS) is a service that translates fully qualified domain names (FQDNs) to IP addresses, and vice versa.

DNS is necessary because, while computers use a numeric addressing scheme to communicate with each other, most individuals prefer to address computers by name. DNS acts as the translator, matching computer names with their IP addresses.

Types of DNS modes

Much of the traffic that flows into and out of your organization must at some point reference a DNS server.

In many organizations this server resides on a separate, unsecured computer. Sidewinder provides the additional option to host the DNS server directly on the firewall, eliminating the need for an additional computer.

Sidewinder offers two main DNS modes:

- **Transparent DNS** — Transparent DNS is designed for simple DNS configurations. The DNS server is on a separate computer, and DNS requests are passed through the firewall using access control rules. This mode is the default DNS configuration for a newly installed Sidewinder.
- **Firewall-hosted DNS** — Firewall-hosted DNS is a more complex DNS configuration that uses the integrated Sidewinder DNS server.



Note: For additional information on DNS, refer to the Internet Systems Consortium website at <http://www.isc.org/>, and the book *DNS and BIND*, Fourth Edition, by Albitz & Liu (O'Reilly & Associates, Inc.).

Related concepts

- [Configuring transparent DNS](#) on page 460
- [Configuring firewall-hosted DNS](#) on page 461

Configuring transparent DNS

In transparent DNS mode, the firewall does not host any DNS servers.

Instead, access control rules allow DNS traffic to pass through the firewall to remote name servers.



Note: Transparent DNS is designed for simple DNS configurations. Complex DNS configurations might require DNS services to be hosted directly on the firewall.

Transparent DNS is configured in two places:

- **Policy > Rules** — Access control rules are required to allow DNS traffic to cross from zone to zone.
 - By default, an access control rule using the DNS application is created that allows all zones to query the name server(s) that you specified during the initial configuration process.
 - If you must allow hosts in one zone to query name servers in another zone, create the appropriate DNS access control rule(s).
- **Network > DNS** — Some firewall processes require DNS resolution. You must define one or more name servers the firewall can send DNS queries to.
 - You can configure unique name servers for each zone.
 - By default, all zones are assigned the name server(s) that you specified during initial configuration. This is sufficient for most services. Notable exceptions are the sendmail and Telnet servers.
 - If you configure a name server for a zone, and that server resides in a different zone, an access control rule is required to allow DNS queries to cross from one zone to the other.

Related concepts

[Modifying the default DNS access control rule](#) on page 460

[Managing transparent name servers](#) on page 460

Modifying the default DNS access control rule

The default DNS access control rule allows hosts in all zones to query the name server(s) you specified during the initial configuration process. This rule is contained by the DNS rule group.

- To allow DNS traffic to reach additional name servers, add network objects for the new name servers to the DNS resolvers netgroup.
- To restrict allowed DNS traffic, you can modify the default DNS access control rule, or disable it and create your own rules.

Managing transparent name servers

If your firewall is configured for transparent DNS, you can add, modify, or delete transparent name servers.

Select **Network > DNS**. The **Transparent DNS Configuration** window appears.



Note: If you want to completely reconfigure your existing DNS configuration (for example, change from transparent DNS to firewall-hosted DNS or vice versa), you must use the **Reconfigure DNS** window.

Related concepts[Reconfiguring DNS](#) on page 477

Configure name servers

Follow these steps to configure the name servers in a list.

- To add a new name server to the list, click **New**. To modify a name server, select the name server and click **Modify**.
- To change the name servers order, select a name server and click the **Up** and **Down** buttons as appropriate.
- To delete a name server, select the name server and click **Delete**.

Add a name server

Add a name server for a zone.

Steps

- 1) In the **Nameserver IP Address** field, type the IP address of the name server.



Tip: For option descriptions, click **Help**.

- 2) Click **OK** and save your changes.

Configuring firewall-hosted DNS

In firewall-hosted DNS mode, DNS servers run directly on the firewall.

This places the DNS server(s) on a hardened operating system, preventing attacks against these servers from penetrating your network. Sidewinder uses Berkeley Internet Name Domain (BIND 9).

Select **Network > DNS**. The **DNS** window appears.

The **DNS** window contains four tabs that allow you to define specific nameserver information.

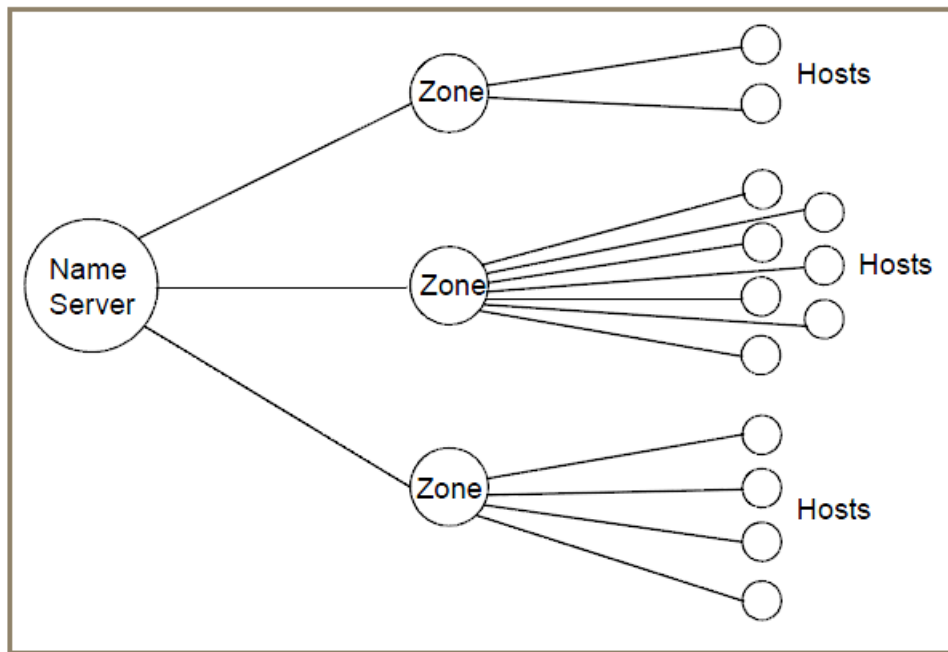
- The **Server Configuration** tab is used to configure general information about a name server..
- The **Zones** tab defines each of the master and slave zones associated with the selected name server.
- The **Master Zone Attributes** tab is used to configure attributes for each master zone defined on the **Zones** tab.
- The **Master Zone Contents** tab defines the hosts associated with each master zone defined on the **Zones** tab..

The following table illustrates the types of DNS objects you can configure and which tab is used to configure each object.

Table 86: DNS objects and the tab used to configure each object

DNS object	Where defined
Name server	Server Configuration tab
Zones (contain forward and reverse lookups)	Zones tab
Hosts (within each zone)	<ul style="list-style-type: none"> Master Zone Attributes tab Master Zone Contents tab

Figure 65: DNS object hierarchy



Related tasks

- [Configure the Server Configuration tab on page 463](#)
- [Configure the Zones tab on page 466](#)
- [Configure the Master Zone Attributes tab on page 468](#)
- [Configure the Master Zone Contents tab on page 472](#)

Choosing a firewall-hosted DNS mode

You can configure firewall-hosted DNS to use a single server or split servers.

- Hosted single server DNS** — In a firewall-hosted single server configuration, the Unbound name server is hosted on the firewall. This mode is appropriate when there is no need to keep the internal network architecture hidden. For example, if your firewall is deployed between two private networks, you might not need to protect the DNS architecture of one network from the other.
- Hosted split server DNS** — In a firewall-hosted split server configuration, two DNS servers are hosted on the firewall:

- Internet name server — This server is bound the external zone. External hosts query this server, which hosts public DNS information.
- Unbound name server — This server is available for use by all internal zones. DNS information hosted by this server is private, and not visible from the Internet.

DNS and IPv6 support

The following options are supported on firewalls that have IPv6 enabled.

- Split Server DNS or Single Server DNS
- IPv4 and IPv6 DNS resolution over either IPv4 or IPv6 addresses
- Complete Admin Console support for IPv6 addresses in records and servers addressing
- Ability to disable IPv6 transport while still serving IPv6 records

Configure the Server Configuration tab

The **Server Configuration** tab is used to define configuration settings for the selected name server.

Related concepts

[Reconfiguring DNS](#) on page 477

Related tasks

[Configure the Zones tab](#) on page 466

[Enable or disable hosted DNS servers](#) on page 475

Modify the Server Configuration tab

Modify the parameters on the **Server Configuration** tab.



Note: To completely reconfigure your DNS settings (for example, change from firewall-hosted single server to split server), click **Reconfigure DNS**.

Steps

- 1) In the **Modify Server For** field, select the name server that you want to modify. (The Internet server is available only if you are using two servers.)



Tip: For option descriptions, click **Help**.

- 2) [Conditional] If you want to disable the selected name server, clear the **Enable Unbound/Internet Domain Name Server** check box. (The Internet Domain Name Server is available only if two servers are defined.) See *Enable and disable hosted DNS servers* for information about the effects of enabling or disabling the servers.



Note: The **File Directory** field displays the location of the files used to store information about the selected server. This field cannot be modified.

- 3) In the **Do Forwarding** field, specify whether the name server will forward queries it cannot answer to another name server. In a split DNS configuration, when modifying the unbound name server this field will default to **Yes** and will forward these unresolved queries to the Internet server (127.x.0.1, where x = the external [or Internet] zone number).

Forwarding occurs only on those queries for which the server is not authoritative and does not have the answer in its cache.

- 4) [Conditional] If you selected **Yes** in the previous step, configure the **Forward Only** field. Specify the following:
- If you select **Yes**, the name server forwards queries it cannot answer to the name servers listed in the **Forward To** list only. This is the default.
 - If you select **No**, the name server forwards the query to the name servers listed in the **Forward To** list. If they cannot answer the query, the name server attempts to contact the root server.
- 5) In the **Forward To** field, specify the alternate name servers that will be used when attempting to resolve a query. This list is consulted only if **Yes** is selected in the **Do Forwarding** field.
- If multiple name servers are defined, the name servers are consulted in the order listed until the query is resolved.
 - In a split DNS configuration, when modifying the unbound name server this list will by default contain four entries for the Internet name server (127.x.0.1, where x = the external [or Internet] zone number).



Note: If you are using a split DNS configuration, do not define additional alternate name servers for the unbound name server. The Internet (or external) name server should be the only alternate name server defined for the unbound name server. To define alternate external name servers, specify them in the Internet name server configuration.

- 6) To add another entry to the list of authorized name servers, click **New** under the **Forward To** list, then type the IP address of the alternate name server. The alternate name servers are consulted if the primary name server cannot resolve a query.
- 7) To delete a name server from the **Forward To** list, highlight the name server you want to delete and click **Delete**.
- 8) [Conditional] To modify an advanced configuration setting for the name server, click **Advanced**.



Note: Only experienced DNS administrators should modify an advanced configuration setting.

- 9) Save your changes.

Add an alternate name server

Add an alternate name server for a zone.

Steps

- 1) In the **Forward to IP Address** field, type the IP address of the alternate name server.



Tip: For option descriptions, click **Help**.

- 2) Click **Add** to save the specified IP address to the list of alternate name servers.
- 3) When you are finished adding alternate name servers, click **Close**.
- 4) Save your changes. The alternate name server has been added.

Modify advanced server options

Modify the notify, allow-query and allow-transfer DNS server options.



Note: Do not change these options unless you are an experienced DNS system administrator.



Note: By default, the options on this window are disabled, meaning *there are no restrictions*. If your organization considers this to be a security risk, you should use these options to limit the amount of interaction this name server has with other devices. Use your organization's security policy as a guide.

Steps

- 1) To enable the **notify** option, select the corresponding check box. Enabling this option allows you to specify whether the master server will notify all slave servers when a zone file changes. The notification indicates to the slaves that the contents of the master have changed and a zone transfer is necessary.
If this field is not selected, the field defaults to **Yes**.



Tip: For option descriptions, click **Help**.

- 2) To enable the **allow-query** option, select the corresponding check box. Selecting this option affects who is able to query this name server. The options are the following:
 - If not selected, all requesters are authorized to query the name server. This is the default.
 - If selected and contains IP addresses, only the requesters defined in the allow-query list are authorized to query this name server. Use the **New** and **Delete** buttons to modify this list.



Note: If you select this option, be sure to include all IP addresses that might need to query the server, such as the heartbeat zones' IP addresses, loopback addresses, etc.

- 3) To enable the **allow-transfer** option, select the corresponding check box. Selecting this option allows you to limit who is authorized to request zone transfers from this name server.
 - If not selected, all requesters are authorized to transfer zones from the name server. This is the default.

- If selected and no IP addresses are added, no requesters are authorized to transfer zones from this name server.
 - If selected and contains IP addresses, only the requesters defined in the allow-transfer list are authorized to transfer zones from this name server. Use the **New** and **Delete** buttons to modify this list.
- 4) Click **OK** to save your changes.

Configure the Zones tab

A DNS server is responsible for serving one or more zones.

A zone is a distinct portion of the domain name space. A zone consists of a domain or a sub-domain (for example, `example.com` or `sales.example.com`). Each zone can be configured as either a master, slave or forward zone on this name server.

Define zone information for a name server

Define zone information for a configured name server.



Note: To completely reconfigure your DNS settings (for example, change from firewall-hosted single server to split server), click **Reconfigure DNS**.

Steps

- 1) In the **Modify Server For** field, select the name server that you want to modify.



Tip: For option descriptions, click **Help**.

- 2) The **Zones** list defines the zones for which the name server is authoritative. This list initially contains a zone entry for each domain and each network interface defined to the firewall. You can add or delete zone entries as follows:
- To add a new zone to the list, click **New** and type the name of the forward or reverse zone you want to add to the list.
 - To delete a zone, highlight a zone and click **Delete**.

Do not delete or modify the following entries:

- Any 127 reverse zones (for example, `0.1.127.in-addr.arpa`). These zones represent local loopback addresses and are required.
- The zone with `0.255.239.in-addr.arpa` in its name. This zone provides multicast support for the Sidewinder failover feature.

There can be two different types of entries in the **Zone** list:

- Reverse zones (for example, `4.3.in-addr.arpa`): This format indicates the entry provides reverse lookup functions for this zone.
- Forward zones (for example, `example.com`): This format indicates the entry provides forward lookup functions for this zone.

The **Related Zones** list displays the zones that are related to the selected zone. For example, if a forward zone is selected, the related reverse lookup zones are displayed. This list cannot be modified.

3) In the **Zone Type** field, specify whether the selected zone is a master zone, a slave zone, or a forward zone, as follows:

- **Master** — A master zone is a zone for which the name server is authoritative. Many organizations define a master zone for each sub-domain within the network. Administrators should only make changes to master zones.



Tip: You should consider defining a matching reverse zone (an **in-addr.arpa** zone) for each master zone you configure.

- **Slave** — A slave zone is a zone for which the name server is authoritative. Unlike a master zone, however, the slave zone's data is periodically transferred from another name server that is also authoritative for the zone (usually, the master). If you select Slave, the **Master Servers** field becomes active. Be sure to use the **Master Servers** field to define the nameserver(s) that will provide zone transfer information for this slave zone. Administrators should not make changes to slave zones.



CAUTION: When changing a zone from slave to master, the Admin Console changes the slave file into a master file and the file becomes the lookup manager for the zone. The DNS server will have no problems understanding and using the new master file. For large zones (class A or B), however, this file might become too complex to be managed properly using the Admin Console. We recommend leaving large zones as slaves on the firewall, or manually modifying these files.

- **Forward** — A forward zone allows you to specify that queries for names in the zone are forwarded to another nameserver.

4) In the **Zone File Name** field, specify the name of the file that is used to store information about this zone. The file is located in the directory specified in the **File Directory** field on the **Server Configuration** tab. We do not recommend changing this name.

5) [Conditional] When **Zone Type** is **Forward**, the **Forwarders** list defines one or more forwarders for a zone. You can add or delete forwarder entries as follows:

- To add a new forwarder to the list, click **New** and type the IP address.
- To delete a forwarder, select that item and click **Delete**.

6) [Conditional] When the **Zone Type** is **Slave**, the **Master Servers** list defines one or more master name servers that are authorized to transfer zone files to the slave zone. You can add or delete server entries as follows:

- To add a new master server to the list, click **New** and type the IP address.
- To delete a master server, highlight a server and click **Delete**.

7) [Conditional] To modify an advanced configuration setting for the selected zone, click **Advanced**.



Note: Only experienced DNS administrators should modify advanced configuration settings.

8) Save your changes.

Related concepts

[Reconfiguring DNS on page 477](#)

Configure advanced zone options

The **Advanced Zone Configuration** window allows you to configure certain options specifically for the selected zone, overriding similar options that might be configured for the global name server (the Unbound or the Internet name server).



Note: Only experienced DNS administrators should modify advanced configuration settings.

Steps

- 1) To enable the **notify** option, select the corresponding check box. Enabling this option allows you to specify whether the master server will notify all slave servers when the zone changes. The notification indicates to the slaves that the contents of the master have changed and a zone transfer is necessary. The name servers that are notified are those defined in the **Zone NS Records** field on the **Master Zone Attributes** tab. If this field is not selected, the field defaults to **Yes**.



Tip: For option descriptions, click **Help**.

- 2) To enable the **allow-query** option, select the corresponding check box. Selecting this option affects who is able to query this zone. The options are the following:
 - If not selected, all requesters are authorized to query the zone. This is the default.
 - If selected and contains IP addresses, only the requesters defined in the allow-query list are authorized to query this zone. Use the **New** and **Delete** buttons to modify this list.



Note: If you select this option, be sure to include all IP addresses that might need to query the zone, such as the heartbeat zones IP addresses, loopback addresses, etc.

- 3) To enable the **allow-update** option, select the corresponding check box. Selecting this option allows you to specify from whom the zone will accept dynamic DNS updates. If this option is selected, only the hosts in the allow-update list are authorized to update this zone. This option is only valid for master zones. Use the **New** and **Delete** buttons to modify this list.

By default the **allow-update** option is not selected, meaning the server will deny updates from all hosts.

- 4) To enable the **allow-transfer** option, select the corresponding check box. Selecting this option allows you to limit who is authorized to request zone transfers from this zone.
 - If not selected, all requesters are authorized to transfer this zone from the name server. This is the default.
 - If selected and no IP addresses are added, no requesters are authorized to transfer this zone from the name server.
 - If selected and contains IP addresses, only the requesters defined in the allow-transfer list are authorized to transfer the zone from the name server. Use the **New** and **Delete** buttons to modify this list.

Configure the Master Zone Attributes tab

Use the **Master Zone Attributes** tab to configure attributes for each master zone defined on the **Zones** tab.

Slave and forward zones are not included on this tab because you can only define attributes for those zones for which the server is the master.

Follow these steps to configure the **Master Zone Attributes** tab.



Note: To completely reconfigure your DNS settings (for example, change from firewall-hosted single server to split server), click **Reconfigure DNS**.

Steps

- 1) In the **Modify Server For** field, select the name server that you want to modify.



Tip: For option descriptions, click **Help**.

The **Master Zones** list defines the zones for which the name server is master. A plus sign (+) will appear in front of any forward lookup zone that contains one or more sub-domains. Click the plus sign to view the sub-domains.

To modify an entry in the list, click the **entry** name. A menu of options used to characterize the selected entry is presented on the right side of the window.



Note: The **Forward Lookup Zone Name/Reverse Lookup Zone Name** field displays the full zone name associated with the entry selected in the **Master Zones** list.

- 2) To modify the **Zone SOA** tab, click the tab and follow the sub-steps below. The fields on the **Zone SOA** tab collectively define one Start Of Authority (SOA) record. An SOA record controls how master and slave zones interoperate.

The **DNS Serial #** field displays the revision number of this SOA record. This field will increment by one each time you modify this zone. Slave zones use this field to determine if their zone files are out-of-date. You cannot modify this field. (See sub-step b for more details.)

- a) In the **DNS Contact** field, specify the name of the technical contact that can answer questions about this zone. The name must be a fully-qualified name, with the @ character replaced by a period (for example, `hostmaster@example.com` becomes `hostmaster.example.com.`).
- b) In the **Refresh** field, specify in seconds how often a slave will check this zone for new zone files. The slave uses the **DNS Serial #** value to determine if its zone files need to be updated. For example, if the slave's DNS serial number is 4 and the master zone's DNS serial number is 5, the slave knows that its zone files are out-of-date and it will download the updated zone files. Values must be positive integers.
- c) In the **Retry** field, specify in seconds how long a slave should wait to try another refresh following an unsuccessful refresh attempt. Values must be positive integers.
- d) In the **Expiration** field, specify in seconds how long a slave can go without updating its data before expiring its data. For example, assume you set this value to 604800 (one week). If the slave is unable to contact this master zone for one week, the slave's resource records will expire. After expiration, queries to that zone will fail. Values must be positive integers.
- e) In the **TTL** field, specify the time to live (TTL) value. This value defines how long a resource record from this zone can be cached by another name server before it expires the record. The value specified here is used as the default in records that do not specify a TTL value. Values must be positive integers.
- f) To add a sub-domain to the selected zone, click **Add Sub**. This button is only available if a forward lookup zone is selected in the **Zones** list. For information on adding a sub-domain, see **Zone SOA: New Forward Lookup Sub-Domain** window.
- g) To delete a sub-domain from the selected zone, click **Delete Sub**. This button is only available if a forward lookup zone is selected in the **Zones** list.

- 3) To modify the **Zone Records** tab, click the tab. This tab contains NS (Name Server) and MX (Mail Exchange) records for forward zones. This tab contains only NS Records for reverse zones.
 - The **Zone NS Records** table contains DNS NS records that indicate what machines will act as name servers for this zone. By default the table contains an entry for the machine you are currently using.
 - To add a Zone NS Records entry, click **New**. In the **NS Record** field, type the domain name associated with this NS record. The name must be a fully qualified name and must end with a period. The name you specify should be a pre-existing domain name that maps to a valid IP address.
 - To delete a Zone NS Records entry, select the entry and click **Delete**.

If this zone is configured to notify all slave servers when a zone file changes, the notify commands are sent to all NS hosts specified here. (See **Zones: Advanced Zone Configuration** window for a description of the **notify** field.)

 - The **Zone MX Records** list is available only if the selected zone entry is a forward lookup entry. It is used to specify entries in the mail exchangers table for the selected zone. The mail exchangers table contains DNS MX records that indicate what machines will act as mail routers (mail exchangers) for the selected domain.
 - To add a Zone MX Records entry, click **New**. Type a fully qualified host name, and a priority level for this record. Valid values are 1–65535. The lower the value, the higher the priority.
 - To delete a Zone MX Records record entry, select the entry and click **Delete**.
 - The **Zone A Record** field is available only if the selected zone entry is a forward lookup entry. It defines a DNS A record (an Address record) for the zone itself. A DNS A record is used to map host names to IP addresses. The address you specify must be entered using standard dotted quad notation (for example 172.14.207.27).
 - The **TXT Record** field is available if the selected zone entry is a forward lookup entry. This optional field allows you to enter comments or additional information about this zone, such as sender id information.
- 4) Save your changes.

Related concepts

[Reconfiguring DNS](#) on page 477

Add a forward lookup sub-domain

Add a forward lookup sub-domain for a zone.

Steps

- 1) In the **Forward Sub-Domain Name** field, type the name of the sub-domain. Do not type a fully qualified name.



Tip: For option descriptions, click **Help**.

For example, assume you have a domain named *example.com* that contains a sub-domain named *west*. You would type *west* in this field rather than *west.example.com*.

- 2) In the **Sub-Domain NS Records** field, specify entries in the **Name Servers** table for this sub-domain. The **Name Servers** table contains DNS NS records that indicate what machines act as name servers for this sub-domain.
 - To add an NS Records entry, click **New**. In the **NS Record** field, type the domain name associated with this NS record. The name must be a fully qualified name and must end with a period. The name you specify should be a pre-existing domain name that maps to a valid IP address.
 - To delete an NS Records entry, select the entry and click **Delete**.
- 3) [Optional] In the **Sub-Domain MX Records** field, specify entries in the mail exchangers table for this sub-domain. The mail exchangers table contains DNS MX records that indicate what machines act as mail routers (mail exchangers) for the sub-domain.
 - To add an MX Records entry, click **New**. Type a fully qualified host name, and a priority level for this record. Valid values are 0–65535. The lower the value, the higher the priority.
 - To delete an MX Records record entry, select the entry and click **Delete**.
- 4) Click **Add** to add the specified sub-domain. Click **Close** to exit the window.

Delete a forward lookup sub-domain

The **Domains in Zone** field lists the domains defined in the zone.

Follow the steps to delete a sub-domain.

Steps

- 1) Highlight the domain you want to delete, then click **Delete Domain**.



Tip: For option descriptions, click **Help**.

- 2) Click **OK** to save your changes. (Click **Cancel** to exit the window without saving your changes.)

Add an NS record

Add an NS record for a zone.

Steps

- 1) In the **NS Record** field, type the domain name associated with this NS record. The name must be a fully-qualified name and must end with a period. The name you specify should be a pre-existing domain name that maps to a valid IP address.



Tip: For option descriptions, click **Help**.

- 2) Click **Add** to add the specified entry to the **Name Servers** table. Click **Close** to exit the window.

Add an MX record

Add an MX record for a zone.

Steps

- 1) In the **MX record** field, type the fully qualified name of the host that acts as the mail exchange for this zone, sub-domain, or host.



Tip: For option descriptions, click **Help**.

- 2) In the **Priority** field, type a priority level for this record. Valid values are 1–65535. The lower the value, the higher the priority (for example, a value of 1 will have a higher priority than a value of 10).
- 3) Click **Add** to save the new record. Click **Close** to exit the window.

Configure the Master Zone Contents tab

The **Master Zone Contents** tab is used to define the hosts that are associated with each master zone.

When you select the **Master Zone Contents** tab, a window similar to the following appears. Select the **Master Zone Contents** tab.



Note: If you are adding a large number of hosts (hundreds or thousands) to a master zone, you might want to consider manually adding the required host information directly to the appropriate DNS files using one of the available editors on the firewall to save time. However, only experienced Sidewinder administrators should attempt this. (Using the manual method will still require you to manually define each host.)

Follow these steps to configure the **Master Zone Contents** tab.



Note: To completely reconfigure your DNS settings (for example, change from firewall-hosted single server to split server), click **Reconfigure DNS**.

Steps

- 1) In the **Modify Server For** field, select the name server that you want to modify.



Tip: For option descriptions, click **Help**.

The fields that are available on this tab will vary depending on whether a zone, a host in a forward lookup zone, or a host in a reverse lookup zone is selected.

- 2) [Conditional] If you are modifying a zone, do the following:
 - a) In the **Master Zones** area, select the zone you want to modify.
 - b) To add a host to the selected zone, click **Add Entry**.
 - If you are adding a host to a forward lookup zone.
 - If you are adding a host to a reverse lookup zone.

- c) To delete a host from the selected zone, click **Delete Entry**. The **Hosts in Zone** field lists all the hosts currently defined within the selected zone. Select the host you want to delete and click **Delete Host**. You can only delete one host at a time.

3) [Conditional] If you are modifying a host in a reverse lookup zone, the following two fields appear:

- **Name (Host portion of IP)** — The field displays the host portion of either the IP address or of the fully-qualified domain name of this entry. You cannot modify this field. If you need to change the name, you must delete the entry from the list, then add the entry back using the new name.
- **Fully-Qualified Domain Name** — This field displays the domain name of the host. You can modify this field by typing in a new value. Be sure to type the fully-qualified domain name of the host.



Note: The **Name** field and the **Fully-Qualified Domain Name Entry** field collectively define a PTR Record for the selected reverse lookup zone. The PTR record is used in a Reverse Addresses table and maps an IP address to a host name.

4) [Conditional] If a host in a forward lookup zone is selected, the following fields appear:

- **Entry Name** — This field defines the host portion of the fully-qualified domain name of this entry.
- **A Record IP** — This field defines a DNS A record (an Address record), which is used to map host names to IP addresses. In this case the field displays the IP address of the selected host. You can modify this field by typing in a new value. The address you specify must be entered using standard dotted quad notation (for example 172.14.207.27).
- **CNAME Rec** — This field defines a DNS CNAME record, which is used to map an alias to its canonical name. The field, if populated, displays the name of the Canonical Record of the selected host. You can modify this field by typing in a new name. The name you specify must be entered using the fully qualified primary name of the domain.



Note: A host in a forward lookup zone requires either an A Record or a CNAME Record.

- **TXT Record** — This field allows you to enter comments or additional information about this zone, such as sender id information.
- **Entry MX Records** — This field is used to specify entries in the mail exchangers table for the selected host. The mail exchangers table contains DNS MX records that indicate what machines will act as mail routers (mail exchangers) for the selected host.
 - To add an MX Records entry, click **New**. Type a fully qualified host name, and a priority level for this record. Valid values are 1—65535. The lower the value, the higher the priority.
 - To delete an MX Records entry, select the entry and click **Delete**.
- **HINFO-Type** — This field provides information about a host's hardware type.
- **HINFO-OS** — This field provides information about a host's operating system.



Note: For security reasons, many organizations elect not to use the HINFO fields.

5) Save your changes.

Related concepts

[Reconfiguring DNS on page 477](#)

Add a forward lookup entry

Add a forward lookup entry for a zone.

Steps

- 1) In the **Entry Name** field, specify the host portion of the fully-qualified domain name of this entry.



Tip: For option descriptions, click **Help**.

- 2) In the **A Record IP** or **AAAA Record** field, specify a DNS A or AAAA record, which is used to map host names to IP addresses, or in the **CNAME Rec** field, specify a DNS CNAME record, which is used to map an alias to its canonical name.
- 3) [Optional] In the **TXT Record** field, enter comments or additional information about this zone, such as sender ID information.
- 4) [Optional] The **Entry MX Records** field lists entries in the mail exchangers table for this host. The mail exchangers table contains DNS MX records that indicate what machines will act as mail exchangers for the host.
 - To add an MX Records entry, click **New**. Type a fully qualified host name, and a priority level for this record. Valid values are 1–65535. The lower the value, the higher the priority.
 - To delete an MX Records record entry, select the entry and click **Delete**.
- 5) [Conditional] The **HINFO-Type:** field provides information about a host's hardware type.
- 6) [Conditional] The **HINFO-OS** field provides information about a host's operating system.



Note: For security reasons, many organizations elect not to use the **HINFO** fields. Click **Add** to save the new entry. Click **Close** to exit this window.

Define a new host for a reverse lookup zone

Configure a new host for a reverse lookup zone.

Steps

- 1) In the **Entry Name** field, specify the host portion of the IP address of this entry.



Tip: For option descriptions, click **Help**.

- 2) In the **Fully-Qualified Name Entry** field, specify the domain name of the host. Be sure to type the fully-qualified domain name of the host.



Note: The **Entry Name** field and the **Fully-Qualified Name Entry** field collectively define a PTR Record for the selected reverse lookup zone. The PTR record is used in a **Reverse Addresses** table and maps an IP address to a host name.

- 3) Click **Add** to save the new entry. Click **Close** to exit this window.

Delete a host

The **Hosts in Zone** field lists all the hosts currently defined within the selected zone.

Steps

- 1) From the list, select the host.



Tip: For option descriptions, click **Help**.

- 2) Click **Delete Host**.



Note: You can only delete one host at a time.

- 3) Click **OK** to save your changes and exit the window.



Tip: Click **Cancel** to cancel your changes.

Enable or disable hosted DNS servers

The firewall-hosted DNS servers start automatically when the firewall starts.

If you disable a firewall-hosted DNS server, your network is affected as follows:

- **Hosted single server DNS mode** — If you disable the unbound DNS server, only connections that use IP addresses still work; those that use host names do not.
- **Hosted split server DNS mode** — Your network is affected differently depending on which server(s) you disable:
 - If you disable the Unbound DNS server, connections that use IP addresses still work; those that use host names do not.
 - If you disable the Internet server, outbound connections that require host names do not work unless the name is already cached (saved) in the unbound name server's database. Connections that use IP addresses work. E-mail is placed in a queue since IP addresses cannot be resolved.
 - If you disable both name servers, connections work only if they use IP addresses rather than host names. Also, e-mail stops flowing, and other errors occur as other parts of the firewall attempt to access the network by name.

To manually enable or disable a firewall-hosted DNS server:

Steps

- 1) Select **Network > DNS**. The **DNS** area appears.



Tip: For option descriptions, click **Help**.

- 2) In the **Modify Server For** area, select the appropriate DNS server.

- 3) Enable or disable the server as necessary.

- To disable the server, clear **Enable [Unbound/Internet] Domain Name Server**.



Tip: The server remains disabled until you manually enable it.

- To enable the server, select **Enable [Unbound/Internet] Domain Name Server**.

Manually edit firewall-hosted DNS configuration files

You can manually edit the DNS configuration files.

- Files with a `.u` extension are for the unbound nameserver, and files with an `.i` extension are for the Internet nameserver.
- Only edit zone files for a master name server. To do so, modify the `/etc/namedb.u/domain-name.db` and `/etc/namedb.i/domain-name.db` files (where *domain-name* = your site's domain name). Never edit slave name server files.

Table 87: DNS server configuration file locations

DNS server	Server configuration file	Zone file directory
Unbound	<code>/etc/named.conf.u</code>	<code>/etc/namedb.u</code>
Internet	<code>/etc/named.conf.i</code>	<code>/etc/namedb.i</code>

To manually edit DNS configuration files:

Steps

- From the command line, log on and enter `srole` to switch to the Admin domain.
The following two steps assume you have zone files named `domain.db` and `reverse-lookup-of-domain.db` in your system. Substitute your file names as required.
- Open the `/etc/namedb.u/domain.db` and `/etc/namedb.i/domain.db` files in a UNIX text editor and make the necessary changes.
- Open the `/etc/namedb.u/reverse-lookup-of-domain.db` and `/etc/namedb.i/reverse-lookup-of-domain.db` files in a UNIX text editor and make the necessary changes.
- Open the `/etc/named.conf.u` and `/etc/named.conf.i` files in a UNIX text editor and make the necessary changes.



Note: If you edit the `/etc/named.conf.*` files to change an existing master zone into a slave zone, you must also manually remove the old zone file in your `/etc/namedb.*` directories.

- If you have added new files, you must change the files to the correct Type Enforcement types. To do this, type the following command and insert the names of the file(s) you edited in steps 2, 3 and 4:

```
chtype DNSx:conf filename
```

- For non-Internet (unbound) zones, in place of `x` type the identifier `u`.

- For the Internet zone, in place of x type the index number of the Internet zone. (Use the region show command to determine the index number.)

6) Increment the serial number after every change to the master files.

7) Validate your changes.

- If you modified a zone file, run the command:

```
/usr/sbin/named-checkzone zonename filename
```

where *zonename* is the domain name of the zone being checked and *filename* is the name of the zone file.

- If you modified a server configuration file, run the command:

```
/usr/sbin/named-checkconf filename
```

where *filename* is the name of the server configuration file, either */etc/named.conf.u* or */etc/named.conf.i*.

8) Enter the following command to restart DNS.

```
cf daemon restart agent=named_unbound
cf daemon restart agent=named_intenet
```



Note: Any files created by named daemons, such as zone backup files or query log files, have types of DNSu:file or DNSx:file.

9) Check */var/log/daemon.log* for any errors.

Reconfiguring DNS

The **Reconfigure DNS** window allows you to completely reconfigure DNS on your Sidewinder.

- Make sure you create a configuration backup before reconfiguring DNS.
- After using the DNS configuration utility, restart the firewall.
- Any active DNS servers on the firewall will be disabled during the reconfiguration process.
- Any prior modifications you have made to your DNS configuration will be lost when you save your changes. You will need to re-apply the modifications.

Change to transparent DNS mode

To switch to transparent DNS mode, click **Reconfigure DNS** on the **DNS** window.

The **Reconfigure DNS: Transparent** window appears.

To reconfigure your DNS settings to use transparent DNS services:

Steps

- 1) In the **New DNS Configuration** drop-down list, select **Transparent**.



Tip: For option descriptions, click **Help**.

- 2) To configure the Sidewinder to use internal name servers:
 - a) Select the **Internal Name Server** check box.
 - b) In the corresponding **IP Address** field, type the IP address of the name server located in the internal zone.
 - c) [Optional] In the **Alternate IP Address** field, type the IP address of an alternate name server.
 - d) In the **Zone** drop-down list, select your internal zone.
- 3) To configure the Sidewinder to use external (Internet) name servers:
 - a) Select the **Internet Name Server** check box.
 - b) In the corresponding **IP Address** field, type the IP address of the name server located in the external (Internet) zone (likely your ISP's name server).
 - c) [Optional] In the **Alternate IP Address** field, type the IP address of an alternate name server.
 - d) Save your DNS settings. A pop-up message appears informing you whether the reconfiguration was successful.



Note: The pop-up message that appears might contain additional information or warnings about your Sidewinder configuration. Please read this message carefully before you click **OK**.

- 4) Restart the firewall: Select **Maintenance > System Shutdown**.

Change to single server hosted DNS mode

To switch to single-server DNS mode, click **Reconfigure DNS** on the **DNS** window. The **Reconfigure DNS: Firewall Hosted (single server)** window appears.

To reconfigure your DNS settings to use hosted single server DNS services:

Steps

- 1) In the **New DNS Configuration** drop-down list, select **Firewall Hosted**.



Tip: For option descriptions, click **Help**.

- 2) Select the **1 Server** radio button.
- 3) In the **Domain** field, verify that the correct domain name appears.

- 4) In the **Authority** field, select one of the following options:
 - **Master** — Select this option if the server you are defining will be a master name server for the specified domain. A master name server contains name and address information for every computer within its zone.
 - **Slave** — Select this option if the server you are defining will be a slave name server for the specified domain. A slave name server is similar to a master name server, except that it does not maintain its own original data. Instead, it transfers data from another name server.
- 5) [Conditional] If you selected **Slave** in the previous step, type the IP address of the master authority server in the **Master IP** field.
- 6) Save your DNS settings. A pop-up message appears informing you whether the reconfiguration was successful.



Note: The pop-up message that appears might contain additional information or warnings about your Sidewinder configuration. Please read this message carefully before you click **OK**.

- 7) Restart the firewall: Select **Maintenance > System Shutdown**.

Change to split server hosted DNS mode

To switch to split server DNS mode, click **Reconfigure DNS** on the DNS window. The **Reconfigure DNS** window appears.

Steps

- 1) In the **New DNS Configuration** drop-down list, select **Firewall Hosted**.
- 2) Select the **2 Servers** radio button.
- 3) To configure the **Unbound** server, do the following:
 - a) In the **Domain** field, verify that the correct domain name appears.
 - b) In the **Authority** field, select one of the following options:
 - **Master** — Select this option if the server you are defining will be a master name server for the specified domain. A master name server contains name and address information for every computer within its zone.
 - **Slave** — Select this option if the server you are defining will be a slave name server for the specified domain. A slave name server is similar to a master name server, except that it does not maintain its own original data. Instead, it transfers data from another name server.
 - c) [Conditional] If you selected **Slave** in the previous step, type the IP address of the master authority server in the **Master IP** field.
- 4) To configure the **Internet** server, do the following:
 - a) In the **Domain** field, verify that the correct domain name appears.

- b) In the **Authority** field, select one of the following options:
 - **Master** — Select this option if the server you are defining will be a master name server for the specified domain. A master name server contains name and address information for every computer within its zone.
 - **Slave** — Select this option if the server you are defining will be a slave name server for the specified domain. A slave name server is similar to a master name server, except that it does not maintain its own original data. Instead, it transfers data from another name server.
 - c) [Conditional] If you selected **Slave** in the previous step, type the IP address of the master authority server in the **Master IP** field.
- 5) Save your changes to reconfigure your DNS settings. A pop-up message appears informing you whether the reconfiguration was successful.



Note: The pop-up message that appears might contain additional information or warnings about your Sidewinder configuration. Please read this window carefully before you click **OK**.

DNS message logging

DNS messages, Type Enforcement errors and process limit errors are logged in the following locations on the Sidewinder.

- `/var/log/audit.raw` — Contains information in the Sidewinder audit format.
- `/var/log/daemon.log` — Contains traditional syslog format messages.

You can view the `audit.raw` file using the **Audit** windows in the Admin Console. The `daemon.log` file can be viewed using any text editor.

Related concepts

[Viewing audit data](#) on page 289

Configuring DNSSEC

You can apply DNS Security Extensions (DNSSEC) to the DNS lookup process on Sidewinder for added security.

DNS is used to resolve host or domain names to IP addresses and to look up other attributes related to a DNS name. DNSSEC is added to validate the authenticity of resolution data provided by another DNS peer.

The associated keys are in a public-private pair, made of the *Key Signing Key* (KSK, a long-term signature key) and the *Zone Signing Key* (ZSK, a short-term signature key). The KSK signs the ZSK, and the ZSK signs the DNS record.

- Firewall is the publisher (master) of the zone — You can generate the public-private keys and enable DNSSEC.
- Firewall is the slave (subscriber) to the zone — You can validate the publisher, enable DNSSEC, and enable validation.



Note: These instructions do not cover DNSSEC Lookaside Validation (DLV).



CAUTION: DNSSEC can only be configured from the command line or a file editor. If you use a file editor, you must restart the firewall. After configuring DNSSEC, do not use the Admin Console DNS windows to configure DNS.

For more information about DNSSEC and its operation, refer to RFC 6781 at <http://www.ietf.org/rfc.html>.

Generate keys and sign the zone file

The keys can be generated and the zone file signed by the firewall that is the publisher of the zone.

Before you begin

The firewall must be using split or single unbound DNS.

Steps

- 1) From the command line, log on and enter `srole`.
- 2) In the same directory of the zone file, create a ZSK for the zone.

```
dnssec-keygen -r /dev/random -a RSASHA256 -b 2048 -n ZONE fw.example.net
```

where *RSASHA256* is your choice of crypto algorithm, *2048* is the size of the key in bits, and *fw.example.net* is the name of the zone.



Tip: Use `/dev/random` to run the process. If the process appears hung, you can use `/dev/urandom` instead. The numbers are less random (making it less secure), but will generate numbers quicker.

- 3) Create a KSK for the zone.

```
dnssec-keygen -r /dev/random -f KSK -a RSASHA256 -b 2048 -n ZONE fw.example.net
```

Creating a KSK creates a public and private key for the zone, starting with a K followed by the name of the zone. These keys are different from the key files generated in the previous step. The public key file ends with the extension `.key` and the private key file ends with `.private`. Leave these keys where they are and make note of the `.key` file as it will be used later.



Tip: You can add an extension `.ksk` to the file for quick identification, as it will be needed for setting up other resolvers that do forward lookups for this zone.

- 4) Add the contents of the public key files (the `.key` files) to the zone file before signing. You can append the contents of the public key files to the zone file:

```
$include /etc/namedb.u/kfw.example.net.+005+48762.key
$include /etc/namedb.u/Kfw.example.net.+005+51346.key
```

where *fw.example.net* is the name of the zone file.

5) Sign the zone file:

```
dnssec-signzone -o fw.example.net -k Kfw.example.net.
+005+51346.key fw.example.net.db Kfw.example.net.+005+48762.key
```

where:

- *fw.example.net* is the name of zone
- *Kfw.example.net.+005+51346.key* is the name of the KSK .key file
- *fw.example.net.db* is the name of zone file
- *Kfw.example.net.+005+48762.key* is the name of the ZSK .key file



Tip: We recommend adding the `-e` flag to specify a date that the keys will expire. If there is no `-e` flag specified, the keys are only valid for 30 days and then the keys need to be re-signed. Refer to the `dnssec-signzone` man page for more information.

Result

When the steps are complete, you will have several files:

- ZSK — Files ending in `.key` and `.private`
- KSK — Files ending in `.key` and `.private`
- Signed zone file — Original zone name file, with `.signed` extension (The signed zone file will be used for DNSSEC on the firewall.)
- An optional DS record you can include — A file starting with `dsset-`

Enable DNSSEC

Configure the firewall to use the signed zone file for the zone.

Steps

- 1) Copy the file that ends with `.signed` into the appropriate `namedb` directory and change the Type Enforcement of the file.

Use either `/etc/namedb.u` or `/etc/namedb.i`. If the zone is hosted on the unbound side, put it in the `/etc/namedb.u` directory.

For the zone index:

- For non#Internet (unbound) zones, type the identifier `u`.
- For the Internet zone, type the index number of the Internet zone. You can use the `show` command to determine the index number.

For example, in the `/etc/named.conf.u` file:

```
chtype DNSu:conf fw.example.net.db.signed
```

where `u` is the zone index and `fw.example.net.db` is the zone file.

- 2) Add `dnssec-enable yes` in the options section of the appropriate `named.conf` file.
For example, in the `/etc/named.conf.u` file find the options section:

```
options {  
    directory "/etc/namedb.u";
```

At the end of that section, enable DNSSEC:

```
        dnssec-enable yes;  
dnssec-enable yes;  
};
```

- 3) Change or add the zone to the appropriate `named.conf` file to use the signed zone file.
For example, in the `/etc/named.conf.u` file:

```
zone "fw.example.net" {  
    type master;  
    file "fw.example.net.db.signed";  
};
```

- 4) Restart the appropriate name server on the firewall:

- For the unbound side:

```
cf daemon restart agent=named-unbound
```

- For the Internet side:

```
cf daemon restart agent=named-internet
```

Result

The firewall is now serving the zone with DNSSEC.

Verify and validate DNSSEC

On a firewall that is a subscriber for the zone, you need to perform several steps to verify or validate your DNSSEC configuration.

You cannot verify DNSSEC from the authoritative server, as it provides only authoritative responses and not authenticated responses. Only resolvers need to validate DNS information.

Steps

- 1) Edit the appropriate `named.conf` file and add `dnssec-enable yes;` and `dnssec-validation yes;` in the options section:

```
options{  
    dnssec-enable yes;  
    dnssec-validation yes;  
    ....
```

- 2) In the same named.conf file, add a new section called trusted-keys, and put the information from the KSK .key file that was generated for the zone into this named.conf file.

Modify the KSK .key file to remove IN DNSKEY, make the zone an FQDN in quotation marks, and put the key in quotation marks.

Original KSK .key file example:

```
fw.example.net. IN DNSKEY 257 3 5
AwEAAadxgsVnDDqkZimOGcm8BRmMYZw8xeJQWN0oeiYdIOPPvqlw9hN1k
aB5JGUilFyBdtJDGbzeS2GuH+wAgaOsRcsHb2JtM4TGnNHnBj95wTclZ
whFqZKwt50uRnPaC7oaCa3Un+wW5xwXydp2PfZYNZkuQW92iCdtTWGm0
HeurtLO3XTWVrDNHRwtZM4jdcyl6Cp8RcexEgZ0Kww5QTYnoOV8=
```

KSK .key file added to the named.conf file:

```
trusted-keys {
    "fw.example.net." 257 3 5
    "AwEAAadxgsVnDDqkZimOGcm8BRmMYZw8xeJQWN0oeiYdIOPPvqlw9hN1k
aB5JGUilFyBdtJDGbzeS2GuH+wAgaOsRcsHb2JtM4TGnNHnBj95wTclZ
whFqZKwt50uRnPaC7oaCa3Un+wW5xwXydp2PfZYNZkuQW92iCdtTWGm0
HeurtLO3XTWVrDNHRwtZM4jdcyl6Cp8RcexEgZ0Kww5QTYnoOV8=";
};
```



Note: The key entry is all on the same line in the named.conf file.

- 3) In the same named.conf file, add the zone as a forwarded zone, with the forwarder being the IP address of the firewall.

For example, if 10.10.1.1 is the IP address of the firewall:

```
zone "fw.example.net" IN {
    type forward;
    forward only;
    forwarders { 10.10.0.10; };
};
```

- 4) Restart BIND on the server.
- 5) Run this command to test DNSSEC:

```
dig +dnssec fw.example.net
```

where *fw.example.net* is the name of the zone.

- 6) Review the flags line in the dig output. Verify that the ad flag indicating Authenticated Data is present and that DNSSEC has been configured properly. If you do not see the ad flag and receive a status of SERVFAIL, then DNSSEC was not set up correctly. Enable DNSSEC logging to determine key issues.

Enable DNSSEC logging

DNSSEC logging can help you determine problems with keys.



Note: Enable DNSSEC logging on the resolving server .

Steps

- 1) Add the following to your named.conf file above the options section:

```
logging{
  channel dnssec_log {
    file "<path of where you want the log file to be located>" size <maximum size the log file will
    grow to
    in megabytes>M;
    print-time yes;
    severity debug 3;
  };
  category dnssec {
    dnssec_log;
  };
};
```

- 2) Restart BIND.

If BIND fails to restart, check the BIND log for why it failed. The information is typically found in the /var/log/daemon.log.

- 3) Run this command to test DNSSEC:

```
dig +dnssec fw.example.net
```

where *fw.example.net* is the name of the zone.

If DNSSEC fails, review the log file you specified in the file setting under the logging section.

Contents

- [Email options](#) on page 487
- [Set up and reconfigure email](#) on page 492
- [Configuring advanced sendmail features](#) on page 494
- [Managing mail queues](#) on page 503
- [Managing email messages sent by firewall](#) on page 506

Configure email services on Sidewinder.

A newly installed firewall is not automatically configured to pass email between zones.



Note: Ensure that DNS is correctly configured before setting up your email services.

Email options

When you run email on a network protected by the Sidewinder, you have two options for getting messages through the firewall.

- **Transparent** — Pass SMTP through the firewall with an SMTP application access control rule
- **Split** — Use sendmail (secure split SMTP servers) on the firewall



Note: If you use the firewall-hosted sendmail servers, you can also use firewall's email anti-virus service.

The two email configuration options are described in the following sections.

How transparent email works

This configuration option allows you to pass SMTP using access control rules (without the sendmail processes running directly on the firewall).

When transparent mode is configured, all inbound (entering the firewall) and outbound (leaving the firewall) email passes by access control rule through the firewall, just as other traffic does.

When using transparent email services, the following email filtering features are available:

- Internal email infrastructure masking
- Message size filtering
- Destination address filtering
- Server reply length checks

- Command filtering
- Header filtering
- Extension filtering
- Global Threat Intelligence



Tip: To enable Global Threat Intelligence in transparent mode, create an access control rule that includes the **SMTP** application, and select **Enable Global Threat Intelligence**.

The transparent mode is best used as a frontline defense together with additional email filtering devices. The firewall can stop a large portion of inbound spam while using a comparatively small amount of system resources. As a result, the workload is substantially reduced on dedicated email filtering devices behind the firewall.

Related concepts

[How McAfee Global Threat Intelligence works](#) on page 128

Related tasks

[Set up and reconfigure email](#) on page 492

Needs of secure split SMTP servers (sendmail)

Hosting sendmail on Sidewinder requires knowledge of both the sendmail application and how the firewall interacts with it.

Read the following sections to learn more.



Note: Secure split mode does not support IPv6.



Note: When using secure split mail, you also have the option of purchasing the anti-virus/anti-spyware service that runs directly on Sidewinder.

Related concepts

[Understanding the secure split SMTP servers](#) on page 488

[Email filtering services for sendmail](#) on page 490

[Configuring virus scanning](#) on page 125

Related tasks

[Set up and reconfigure email](#) on page 492

Understanding the secure split SMTP servers

The secure split SMTP servers option provides two sendmail servers running directly on the firewall, each supported on its own zone: an external zone and one non-Internet zone that you choose.

The firewall's sendmail servers will route email through the firewall only for these two zones.

This configuration protects your internal mail host from malicious attacks, and offers a variety of additional email-handling options. When using secure split SMTP servers, the firewall's external sendmail server is the mail host to which all external SMTP hosts will connect. The firewall's internal sendmail server will connect with internal mail hosts in its same zone.



Note: Your internal mail host must run email software that can accept incoming messages from, and send outgoing messages to, your Sidewinder. This system might be running sendmail or some other email package such as Microsoft Exchange or cc:Mail with an SMTP gateway.

The necessary configuration files and everything you need to run the firewall-hosted mail server are automatically set up for you, such as:

- The three mail domains: *mtac*, *mtaX*, and *mtaY* (where *X* = the number of the external zone, and *Y* = the number of an internal zone), are in place. Sendmail is already configured to route email among these three sendmail servers.
- Mail addressed to users on your internal network will be forwarded to the mail host you specify in the **Reconfigure Mail** window.
- Messages that are sent to the person administering an email system are generally addressed to “postmaster.” During the Quick Start Wizard (initial configuration), you set up an administrator's account. Postmaster messages are automatically routed to that administrator's firewall-hosted email account. (we recommend that all administrators redirect their local email to a non-firewall-hosted email account.)



Note: You will need to configure your internal mail server to forward non-local email to the firewall. This procedure differs depending on the type of email program your network runs. Refer to your email software's documentation for details.

When you configure secure split SMTP servers, there are three separate sendmail servers that each have a different purpose:

- **Local** — The local server handles email that is sent directly from the firewall. For example, if an administrator sends an email message from the firewall, it is sent through the local server. This sendmail process runs in the *mtac* domain and forwards all email to the firewall's internal network.
- **Internal** — The internal server runs in the *mtaY* domain, where *Y* is the zone index of an internal zone that you specify when running Reconfigure Mail. This internal sendmail server *receives* email from one of three sources:

- A host on the internal network
- A sendmail process transferring email from the local sendmail server
- A sendmail process transferring email from the external sendmail server

This internal sendmail server *delivers* email to one of three destinations:

- If the message is for a user local to the firewall, such as an administrator with a mailbox on the firewall, it delivers the message to the user's mailbox using the `mail.local` program.
 - If the message is for a user on the internal network, it connects to the mail host on the internal network and delivers the email there.
 - If the message is not for either of the above, it assumes the message is for an external user and transfers the message to the external zone for that user.
- **External** — The external server runs in the *mtaX* domain, where *X* is the zone index of the Internet zone. This sendmail server *receives* email from one of two sources:
 - Host on the external network
 - Sendmail process transferring email from the internal sendmail server

The external server *delivers* email to one of two destinations:

- If the message is for an external user, it connects to an external host and delivers the email there.
- If the message is for a user local to the firewall (such as an administrator) or for a user on the internal network, it transfers the email to the internal zone for delivery to that user.

When using secure split SMTP servers, all email for a user local to the firewall goes to the internal *mta* domain for delivery. Local delivery does not take place in the external *mta* domain or the *mtac* domain.

Keep in mind the following when using this option:

- The firewall runs three separate sendmail servers (as described in the previous section).
- Type Enforcement restricts sendmail so that its security flaws cannot be exploited. For example, firewall administrators cannot execute shell scripts or other executables through sendmail, as they could on a standard UNIX system.
- Aliases allow users to send their email to another mailbox that might be at a different location. For example, firewall administrators might choose to redirect their email to a mailbox located on the internal network so they receive all of their email in one place. Administrators can use the `/etc/mail/aliases` file, but this file cannot contain commands to run other programs, such as program mailers (for example, `procmail`).
- If a server is too busy to send a message, or if the machine it is sending email to is not responding, the messages are sent to a mail queue. The firewall has a separate queue for each sendmail server: `/var/spool/mqueue.#`, `/var/spool/mqueue.#`, and `/var/spool/mqueue.c` (# = the zone number).



Note: If email cannot be delivered on the first attempt, it is placed in a queue. By default, the system checks the queues every 30 minutes and attempts redelivery.

You can check if there are messages in the mail queues by following the steps described in *Managing mail queues*.

Mail is an extremely complex subject and can require a great deal of effort to configure. If you want additional information on managing email, the best resource is the book *sendmail* by Bryan Costales (O'Reilly & Associates, Inc.).

Related tasks

[Set up email aliases for administrator accounts](#) on page 506

Email filtering services for sendmail

The secure split SMTP servers option provides the ability to do on-box email filtering. To filter messages, you must create access control rules using a sendmail server and a Mail Application Defense with the filter options configured.

The following email filtering services are available:

Global Threat Intelligence spam filtering

Global Threat Intelligence is a reputation service that filters incoming email connections and then provides precise information about an email sender's reputation based on its IP address.

The Global Threat Intelligence reputation service is a tool for reducing the amount of spam that reaches your organization's inboxes. Global Threat Intelligence provides spam protection for SMTP and sendmail.

To enable Global Threat Intelligence for sendmail, select **Perform GTI filtering on inbound mail** on the **GTI Reputation** window.

Related concepts

[How McAfee Global Threat Intelligence works](#) on page 128

MIME/Virus/Spyware filtering

The MIME/Virus/Spyware Application Defense options allow you to perform the following actions.

- Allow, deny, or scan specific types of MIME elements and specific file extensions
- Configure how to handle infected files
- Specify file attachment size restrictions (per message, not per attachment)
- Determine whether email messages will be scanned as a whole (entire message is allowed or denied) or in segments (attachments might be dropped if they do not meet filtering criteria, but the acceptable portions of the email message will still reach the recipient)
- Reject all email if scanning services become unavailable

You must first configure the virus scanner, then apply virus scanning per-rule using the access control rule's application defense.

Related concepts

[Configuring virus scanning](#) on page 125

Related tasks

[Configure the default filtering action](#) on page 187

Keyword search filtering

The Keyword Search filter allows you to filter email messages based on the presence of defined key words (character strings).

Configure size limitations for email messages

The size filter performs a check on email messages for the number of bytes the message contains, including the message header. Messages that equal or exceed the specified size you specify will be rejected.

Anti-relay controls

Anti-relay control uses access control to prevent your mail host from being used by a hacker as a relay point for spam to other sites. This option is automatically enabled for all Mail defenses and cannot be disabled.

Set up and reconfigure email

The **Reconfigure Mail** window is used to configure either firewall email option.

Steps

1) Select **Policy > Application Defenses > Defenses > Mail (Sendmail)**.

2) Click **Sendmail Properties**.



Tip: For option descriptions, click **Help**.

3) Click **Reconfigure Mail**. The **Reconfigure Mail** window appears.

Before you make any changes you should be aware that if you manually edited any sendmail configuration files, changing your email configuration in the **Reconfigure Mail** window will overwrite the changes you made.

To establish or change your email configuration:

a) Verify that DNS is configured correctly.

b) Make a configuration backup before you change your email configuration: Select **Maintenance > Configuration Backup**.

c) On the **Reconfigure Mail** window, expand the **New SMTP Mode** drop-down list and select the email configuration mode you want to configure. The current mode is listed in the **Current SMTP Mode** field. The following options are available:

- **Transparent** — Use this option if you want to use access control rules to allow SMTP through the firewall. If you select this option, only the files necessary to send administrative messages (including firewall-generated alerts, messages, and logs) will be configured.
- **Secure Split SMTP Servers (firewall-hosted)** — Use this option to use the firewall-hosted sendmail server(s). This configuration allows you to take advantage of additional sendmail features, including header stripping, email routing, aliases, and masquerading.

4) In the **Internal SMTP Zone** field, select the zone in which the internal SMTP server resides.

- 5) In the **Internal SMTP Mail Server** field, type the fully qualified name of your site's internal SMTP server. Do not use simple host names or IP addresses.
- 6) Click **Save** in the toolbar (or click **Apply** if you are accessing this window from the Mail (Sendmail) Application Defense) to reconfigure your email mode. A confirmation window appears when the reconfiguration process is complete.
- 7) [Conditional] If you accessed Reconfigure Mail from the Mail (Sendmail) Application Defense, click **Close** to return to the sendmail server **Properties** window.
- 8) Select **Policy > Access Control Rules** and create or modify the necessary access control rules:
 - If you select **Transparent**:
 - Create two access control rules: one for inbound email and one for outbound email.
 - Use the **SMTP** application.
 - Use two **Mail (SMTP proxy)** application defenses: one for inbound traffic and one for outbound traffic, each with direction-appropriate settings.
 - If you select **Secure Split SMTP Servers**:
 - Create two access control rules: one for inbound email and one for outbound email.
 - Use the **Sendmail Server** application.
 - The rules' destination zone must be **<Any>**. The endpoint must also be **<Any>**.
 - Use two **custom Mail (Sendmail) Application Defenses**: one for inbound traffic and one for outbound traffic, each with direction-appropriate settings.



Note: If you are changing your email configuration, you will need to update or replace your existing email rules to reflect the new configuration.

- 9) Save your changes.

Result

The firewall now has a new email configuration.

- If you selected **Transparent**, email management is primarily handled off-box and does not require changes to any Sidewinder mail files.
- If you selected **Secure Split SMTP Servers** and are an experienced email administrator, you might want to edit the configuration files.

Related concepts

[Configuring access control rules](#) on page 197

[Configuring advanced sendmail features](#) on page 494

[Editing sendmail files on Sidewinder](#) on page 498

Configuring advanced sendmail features

Once you run Reconfigure Mail to set up hosted email and create the appropriate access control rules, the basic mail services are enabled.

However, sendmail provides several additional features that you might choose to configure. Of those listed here, email routing, header stripping, and the RealTime Blackhole list are the most popular additional sendmail features. The details for implementing these features are described in the sections that follow.

- **Blackhole list** — Enables you to eliminate unwanted and unsolicited email. The types of spam control you might implement include use of a Realtime Blackhole list, Promiscuous Relaying, and so on.
- **Authenticating** — Enables you to force authentication through the use of a public key.
- **Filter mail based on the user** — Enables you to allow or deny email based on a specific user or users.
- **Header stripping** — Enables you to remove header information from an outbound message to conceal internal host information from the outside world.
- **Mail routing** — Enables you to reroute email from one domain name to another domain name by editing the mailertable files.
- **Masquerading** — Enables you to transform a local host address in the header of an email message into the address of a different host.



Tip: You can also configure aliases for email accounts. Creating aliases for the firewall administrator accounts is particularly useful because system messages sent to these accounts can, if left unattended, fill up the firewall's hard drive.

Related concepts

[Enabling sendmail TLS](#) on page 495

Related tasks

[Configure sendmail to use the RealTime Blackhole list](#) on page 494

[Configure sendmail to strip message headers](#) on page 497

[Configure sendmail to hide internal email addresses](#) on page 501

[Allow or deny email on a user basis](#) on page 496

Configure sendmail to use the RealTime Blackhole list

Sendmail is able to use the services of the RealTime Blackhole List (RBL), a list of known spam domain names.

You must subscribe to a RBL to use this option. After you subscribe to a RBL and configure sendmail to use the list, the mail server checks each email message against the RBL. Any email message originating from a domain in the list will be rejected.

To configure the firewall to use a Realtime Blackhole List:

Steps

- 1) In the Admin Console, select **Policy > Application Defenses > Defenses > Mail (Sendmail)**. The **Mail (Sendmail)** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **Sendmail Properties**. The **Application Defenses: Sendmail Properties** window appears.



Note: Separate configuration files are maintained for each zone.

- 3) In the external zone list, select **M4 Config File**, then click **Edit File**.



Tip: Before making any changes, select **File > Backup** and create a backup of this file.

- 4) Add the following line to the file.

```
FEATURE(`dnsbl', `domain')dnl
```

The *domain* that you enter in the above line will depend on the type of service for which you have subscribed.

- 5) Save and then close the file.
- 6) Click **OK**. The **Application Defenses: Sendmail Properties** window closes.
- 7) Click **Save** to save the configuration changes and rebuild the configuration and database files. This will also automatically restart the sendmail servers.



Note: If at a command prompt, use `cf sendmail rebuild` and `cf daemon restart agent=sendmail`.

Result

Now when the firewall receives email, it will query the RBL to see if the sender's domain is on the list. If the domain is a match, sendmail rejects the message.

Enabling sendmail TLS

The sendmail implementation of RFC 2487, SMTP over TLS, is supported on Sidewinder.

Sendmail can act as either a client or server in a TLS session.

- When acting as the server, it advertises the STARTTLS feature in the response to the EHLO command, then responds positively to the subsequent STARTTLS command.
- When acting as the client, it issues the STARTTLS command if the remote server advertises STARTTLS on the EHLO response.

In both cases, after the STARTTLS command and positive response, the client and server negotiate a TLS session.



Note: As part of the implementation, sendmail TLS also enforces FIPS 140-2 mode.

For more information on enabling sendmail TLS, see Knowledge Base article [9003](#).

Allow or deny email on a user basis

Sendmail will allow or deny email on a domain basis. However, you can also instruct sendmail to allow or deny email to/from specific users, IP addresses, and subnets within a domain.

To do this, follow the steps below:

Steps

- 1) In the Admin Console, select **Policy > Application Defenses > Defenses > Mail (Sendmail)**. The **Mail (Sendmail)** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **Sendmail Properties**. The **Application Defenses: Sendmail Properties** window appears.



Note: Separate configuration files are maintained for each zone.

- 3) Select the **Access Table** file for the appropriate zone and click **Edit File**.



Tip: Before making any changes, select **File > Backup** and create a backup of this file.

- 4) Add the specific allow (**RELAY**), deny and notify the sender (**REJECT**), and/or deny without notifying the sender (**DISCARD**) information to the access table.

For example, if you want to allow email addressed to Lloyd and Sharon but deny email addressed to everyone else, you would add the following lines:

```
# Allow email addressed to these usersTo:Lloyd@example.com
RELAYTo:Sharon@example.com
RELAY# Deny email for everyone elseTo:example.com REJECT
```



Note: For additional information, see the README file in the `/usr/share/sendmail` directory on the firewall.

- 5) Save and then close the file.
- 6) Click **OK**. The **Application Defenses: Sendmail Properties** window closes.
- 7) Click **Save** to save the configuration changes and rebuild the configuration and database files. This will also automatically restart the sendmail servers.



Note: If at a command prompt, use `cf sendmail rebuild` and `cf daemon restart agent=sendmail`.

Result

Mail from those specified users, IP addresses, and subnets will now be handled as indicated in the file.

Configure sendmail to strip message headers

During the normal operation of sendmail, the path a message traces is appended to the message by each host through which the email passes. This enables internal host names and IP addresses to be allowed beyond the firewall.

Header information can only be removed for outbound email. Therefore, you should only enable header stripping in the external (destination) zone for a message. If you configure header stripping in the source zone of a message, header stripping will not happen for that message.

You can configure sendmail to strip (remove) or scrub (change to a different value) the following headers from messages leaving the firewall:

- Received (stripped)
- X400-received (stripped)
- Via (stripped)
- Mail-from (stripped)
- Return-path (stripped)
- Message-id (scrubbed)
- Resent-message-id (scrubbed)



Note: Stripping the headers will **not** alter the To and From hosts. The To and From hosts can be eliminated using access control rules in the **sendmail** configuration file. You can also modify the To and From hosts using masquerading or by editing the domain tables.

To configure sendmail to strip or scrub headers:

Steps

- 1) In the Admin Console, select **Policy > Application Defenses > Defenses > Mail (Sendmail)**. The **Mail (Sendmail)** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **Sendmail Properties**. The **Application Defenses: Sendmail Properties** window appears.



Note: Separate configuration files are maintained for each zone.

- 3) Select the **M4 Config File** in the external zone list and click **Edit File**.



Tip: Before making any changes, select **File > Backup** and create a backup of this file.

- 4) Locate the `C{STRIP_DOMAINS}` line in the file and append the domain name on which to perform header stripping. For example:

```
C{STRIP_DOMAINS} domainx
```

where *domainx* = the domain name on which to perform header stripping.

You can define multiple domains by entering multiple domain names on one line (for example, `C{STRIP_DOMAINS} abc.com xyz.com`).



Note: `STRIP_DOMAINS` contains the list of domains that will trigger header stripping. Each message processed by `sendmail` in the external zone will be subjected to header stripping if it is received from a domain in this list.

- 5) Save and then close the file.
- 6) Click **OK**. The **Application Defenses: Sendmail Properties** window closes.
- 7) Click **Save** to save the configuration changes and rebuild the configuration and database files. This will also automatically restart the sendmail servers.



Note: If at a command prompt, use `cf sendmail rebuild` and `cf daemon restart agent=sendmail`.

Editing sendmail files on Sidewinder

When using the secure split SMTP servers, the sendmail configuration information is stored in *sendmail.cf* files.

These files contain information such as which delivery agents to use and how to format message headers. You should change your configuration options only if you are directed to do so by [Forcepoint support](#), or if you are an experienced sendmail user and want to customize the files for your site.

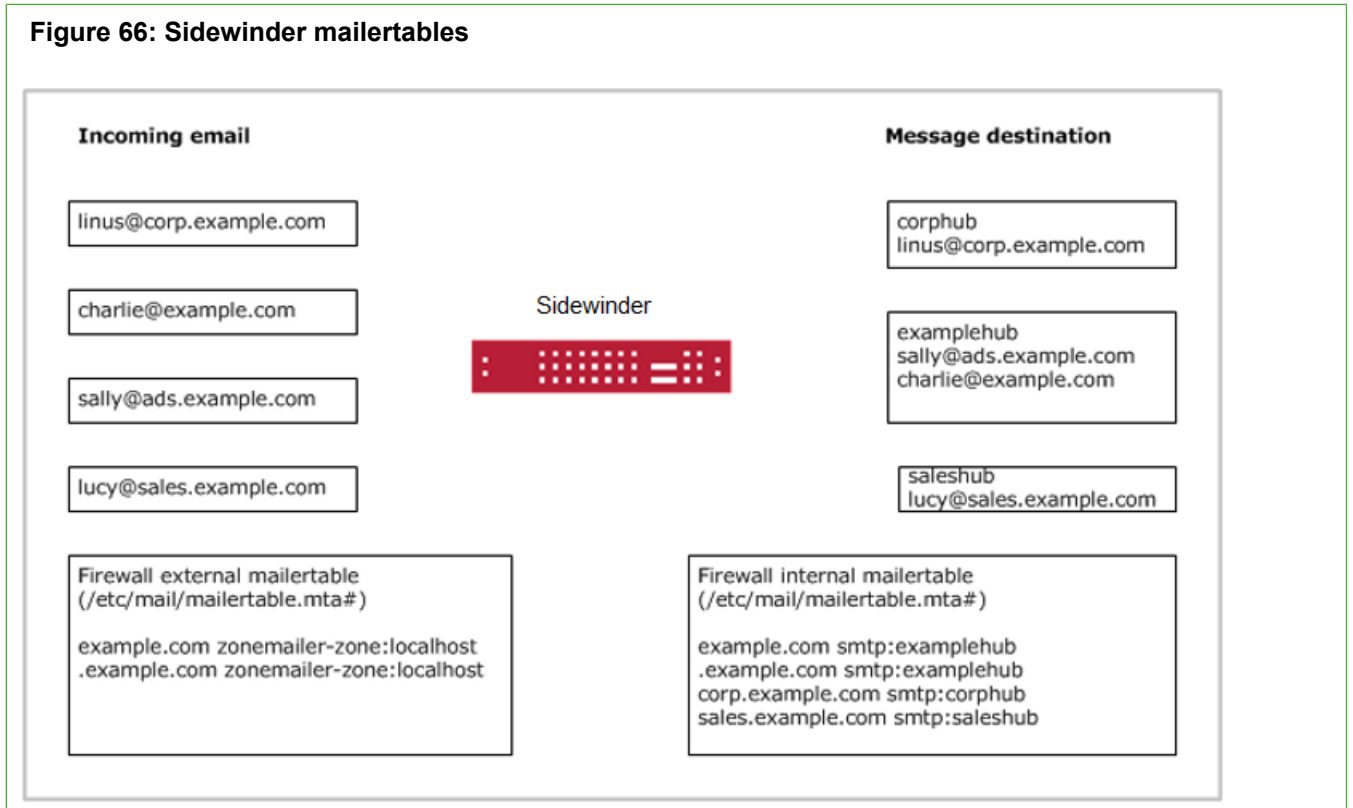
Sendmail allows you to create configuration files using macros written for the `m4` preprocessor. For more information about these macros, refer to the *UNIX System Administration Handbook*. You can also refer to the book *sendmail* by Bryan Costales (O.Reilly & Associates, Inc.).

The firewall sets up two mailertables for you: one internal and one external.

- The external mailertable, `/etc/mail/mailertable.mta#` (`#` = the number of the external zone), processes the email and directs it to the internal mailertable.
- The internal mailertable, `/etc/mail/mailertable.mta#` (`#` = the number of an internal zone), sorts the email by host name, and sends the email to the correct internal mail host.

The following figure shows an example of the route that incoming email messages travel along.

Figure 66: Sidewinder mailtables



The recommended method of editing the mail files is to change the sendmail server's properties using the Admin Console. This opens a file editor that knows to automatically rebuild and restart the sendmail server when you save a file. To edit the mail configuration files using this method, see **Sendmail Properties** window.

To edit the mail configuration files using this method:



CAUTION: Only experienced administrators should modify sendmail configuration files.

- 1) In the Admin Console, select **Policy > Application Defenses > Defenses > Mail(Sendmail)**. The Mail (Sendmail) window appears.
- 2) Click **Sendmail Properties**. The **Application Defenses: Sendmail Properties** window appears.

Modify a configuration file

You can modify a configuration file in the appropriate zone configuration file list. There are separate files for each sendmail server running on the firewall.

Steps

- 1) Select the configuration file you want to modify. You can edit the following files.



Tip: Before making any changes, select **File > Backup** and create a backup file. Also, for best results, do not edit these files with any other file editor, as those editors will not automatically rebuild and restart the sendmail server.

- **Access Table** — This file defines anti-relaying and anti-spamming policies for the SMTP server.
- **Aliases file** — (Available only in the internal zone.) This file defines the email aliases that are used to redirect email to another person or location.
- **Alternate Host Names file** — This file identifies alternate host names by which the firewall is known. email addressed to any of the alternate names is treated as local email by the firewall.
- **Domain Table** — This file provides a mapping from an old domain name to a new domain name. For example, you might modify this file if your organization's external domain name changes.
- **M4 Config file** — This file defines the initial sendmail configuration. Modify this file as needed to account for your site-specific requirements.
- **Mailer Table** — This file maps a domain to a mail relay that is responsible for email delivery in that domain.



Note: Only edit mail configuration files if it is necessary for your site's email functionality.

- 2) Save and then close the file.
- 3) Open the appropriate mailertable file and edit as necessary.



Note: Only edit mailertable files if it is necessary for your site's email functionality.

The mailertable files are named `/etc/mail/mailertable.mta#` (# = the appropriate zone number).

- 4) Enter the correct domain, mailer, and host in the following format:

```
domain <tab> mailer:host
```

On the internal side of the network, the mailertable appears as:

```
.example.net <tab> smtp:examplehub
example.net <tab> smtp:examplehub
corp.example.net <tab> smtp:examplehub
sales.example.net <tab> smtp:examplehub
```

On the external side of the network, the mailertable should appear as:

```
example.net <tab> zonemailer-zone:localhost
.example.net <tab> zonemailer-zone:localhost
```

where *zone* = the external zone number and *Y* = the internal (trusted) zone number.

The entries that begin with a dot (.) act as a wildcard, matching anything with that domain name. The entries that do not begin with a dot match the full domain name. See the `/usr/share/sendmail/README` file for more information on creating mailertables.

- 5) Save and then close the file.
- 6) Click **Save** to save the configuration changes and rebuild the configuration and database files. This will also automatically restart the sendmail servers.



Note: If at a command prompt, use `cf sendmail rebuild` and `cf daemond restart agent=sendmail`.

The firewall updates sendmail with your changes and is then ready to process email. This window also has a shortcut to the **Reconfigure Mail** area.

Related tasks

[Set up and reconfigure email on page 492](#)

Configure sendmail to hide internal email addresses

Occasionally, you might use domain names on your internal network that you do not want the rest of the Internet to know about.

You can instruct sendmail to change the header information so that it hides internal domains before relaying the email on to the final destination. This is called *masquerading*. Masquerading also involves modifying the 'From' or 'From:' field before the email is relayed. To do this, follow the steps below:



Tip: Using `masquerade_entire_domain` field is effective, but it leaves open the possibility of showing internal addresses that are included on the message (such as the Cc or To fields). Use `masquerade_envelope` field to masquerade all addresses in the envelope containing the domain using the specified domain.

Steps

- 1) In the Admin Console, select **Policy > Application Defenses > Defenses > Mail (Sendmail)**. The **Mail (Sendmail)** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **Sendmail Properties**. The **Application Defenses: Sendmail Properties** window appears.



Note: Separate configuration files are maintained for each zone.

- 3) Select the **M4 Config File** for the Internet zone (generally the external zone).



Note: Before making any changes, select **File > Backup** and create a backup.

- 4) Identify the domains you want hidden:

- a) Locate the **MASQUERADE_DOMAIN** section. The default looks like this:

```
nl # MASQUERADE_DOMAIN(`hide_me.acme.com hide_me_too.acme.com')dn1
```

- b) Uncomment the line by deleting "dn1 #".
- c) Change the listed domains to the domain or domains that you want to hide. For example, `hide_me.acme.com hide_me_too.acme.com' becomes 'sales.example.net'.

- 5) Enter the domain you want to show:

- a) Locate the **MASQUERADE_AS** section. The default looks like this:

```
nl # MASQUERADE_AS(`newdomain.com')dn1
```

```
dn1 # FEATURE(`masquerade_entire_domain')dn1
```

```
dn1 # FEATURE(`masquerade_envelope')dn1
```

- b) Uncomment the section by deleting each 'dn1 #'.
- c) In the **MASQUERADE_AS** line, change the listed domain to the domain that should replace all internal domains. For example, `newdomain.com' becomes 'example.net'.

- 6) Save and then close the file.

- 7) Click **OK**. The **Application Defenses: Sendmail Properties** window closes.

- 8) Click **Save** to save the configuration changes and rebuild the configuration and database files. This will also automatically restart the sendmail servers.



Note: If at a command prompt, use `cf sendmail rebuild` and `cf daemon restart agent=sendmail`.

Managing mail queues

If a sendmail message cannot be delivered (for example, if the destination system is down), messages are temporarily placed in queues until they can be delivered.

There are separate queues for each server: `/var/spool/mqueue.c` (local) and `/var/spool/mqueue.#` for the Internet and the trusted zones. The following sections explain how to view email, how to change some of the basic queue settings, and how to manually force sendmail to attempt to deliver queued email.



Tip: You should check the queues periodically. If there are a lot of messages that are several days old, you might have a problem with your system or its configuration.

Viewing the mail queue

Use the `mailq` command to view the mail queue output.

The output of this command lists the messages currently in the queue you chose, along with information about each message. Each message is assigned a unique identification number, which is shown in the first column. In the following example, the external queue shows a message still in queue due to some temporary error. The internal queue shows a valid message ready to be delivered or possibly currently being delivered. The `common_sendmail` queue shows no email queued up which should normally, but not always, be the case.

```
Listing the external Queue
                /var/spool/mqueue.1 (1 request)
-----Q-ID----- --Size-- -----Q-Time-----
-----Sender/Recipient-----
kA6M17qb008045      4 Mon Nov 6 16:01 me@mydomain.com
                    (Deferred: Connection refused by yourdomain.com.)
                    you@yourdomain.com
                    Total requests: 1
Listing the internal Queue
                /var/spool/mqueue.2 (1 request)
-----Q-ID----- --Size-- -----Q-Time-----
-----Sender/Recipient-----
kA6M4gd8008175      4 Mon Nov 6 16:04 admin@fwdomain.com
                    adminuser@internaldomain.com
                    Total requests: 1
Listing the common_sendmail Queue
                /var/spool/mqueue.c is empty
                    Total requests: 0
```

Change how long a message waits between delivery attempts

By default, undelivered email messages remain in the mail queues 30 minutes before another delivery attempt is made.

If you want to change the length of time email messages remain in the mail queues before another delivery attempt is made, do the following:

Steps

- 1) In the Admin Console, select **Policy > Application Defenses > Defenses > Mail (Sendmail)**. The **Mail (Sendmail)** window appears.

- 2) Click **Sendmail Properties**. The **Application Defenses: Sendmail Properties** window appears.



Note: Separate configuration files are maintained for each zone.

- 3) Select the **M4 Config File** for the zone that is running sendmail, and click **Edit File**.



Tip: Before making any changes, select **File > Backup** and create a backup of this file.

- 4) Scroll to the **Set the Queue Interval** area and edit the following line:

```
define(`confQUEUE_INTERVAL', `Xm')dnl
```

where:

X is the amount of time that the message remains in the queue before an attempt is made to resend the message.

m indicates that the time will be measured in minutes. You can also use other time measurements, such as seconds (s), hours (h), days (d), etc.



Note: The default value is 30 minutes.

- 5) Save and then close the file.
- 6) Click **OK**. The **Application Defenses: Sendmail Properties** window closes.
- 7) Click **Save** to save the configuration changes and rebuild the configuration and database files. This automatically restarts the sendmail servers.

Result

The time a message waits before sendmail attempts to deliver it is changed.

Manually attempt to deliver queued messages

Occasionally, you might need to attempt to send all queued messages immediately, instead of waiting for them to be pushed automatically.

This process is called *flushing* the mail queue. If you want to force sendmail to attempt to deliver its queued messages, do the following:

Steps

- 1) At a firewall command prompt, enter the following command to change to the Admn role:
srole
- 2) Instruct sendmail to manually attempt to deliver email in one or more mail queues:
 - `cf sendmail flush` — flushes all three queues
 - `cf sendmail flush queue=zonename` — flushes only the queue for that zone
 - `cf sendmail flush queue=common` — flushes the queue containing email sent by the firewall, such as system updates and alerts

Result

The firewall immediately attempts to send all email in the queue.

Change how long a message waits before it is returned to its sender

By default, undelivered email messages remain in the mail queues 5 days before they are returned to their senders as undeliverable and deleted from the queue.

If you want to change the length of time email messages remain in the mail queues before they are considered undeliverable, do the following:

Steps

- 1) In the Admin Console, select **Policy > Application Defenses > Defenses > Mail (Sendmail)**. The **Mail (Sendmail)** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **Sendmail Properties**. The **Application Defenses: Sendmail Properties** window appears.



Note: Separate configuration files are maintained for each zone.

- 3) Select the **M4 Config File** for the zone that is running sendmail, and click **Edit File**.



Tip: Before making any changes, select **File > Backup** and create a backup of this file.

- 4) Locate the **Set the Queue Interval** area and edit the following line:

```
define(`confTO_QUEUERETURN', `Xd')dnl
```

where:

X is the amount of time that the message remains in the queue its sender is notified that it was undeliverable and the message is deleted.

d indicates that the time will be measured in days. You can also use other time measurements, such as seconds (s), minutes (m), hours (h), etc.

The default value is 5 days.

- 5) Save and then close the file.
- 6) Click **OK**. The **Application Defenses: Sendmail Properties** window closes.
- 7) Click **Save** to save the configuration changes and rebuild the configuration and database files. This automatically restarts the sendmail servers.

Result

The time an undelivered message waits before sendmail returns it to its sender is changed.

Managing email messages sent by firewall

Sidewinder sends status updates and alerts to root and administrator accounts.

By default, these accounts are hosted on the firewall and must be checked using a command line session. If you want to redirect email from your administrators' firewall mailboxes to a different destination, you can edit the `/etc/mail/aliases` file. The following sections provide information on how to create email aliases or access the email messages directly on the firewall.

Set up email aliases for administrator accounts

On the firewall, messages and other files are often emailed to system users such as `root` and `postmaster`. To redirect these system messages to an external account, you can set up an alias.



Tip: Remember to update aliases when there are personnel changes.

Aliases are stored in the `/etc/mail` directory, which can be accessed through the sendmail server. Do the following to set up an email alias for system users:

Steps

- 1) At a firewall command prompt, enter the following command to change to the Admn role:

```
srole
```

- 2) Using a file editor, open `/etc/mail/aliases`.
- 3) Locate the root line in the file. The default, root, is automatically aliased to the administrator account created during the Quick Start Wizard and looks like this:

```
#root:username
```

- 4) Uncomment the line by deleting the #, and then replace the existing address with the off-box email address of the person who will receive system messages. If you want to add multiple accounts, separate them with commas and do not include spaces.

The line now looks like this:

```
root: username_a@example.com,username_b@example.com
```

By default, all other system roles are aliased to root, and email sent to those accounts will also be sent to the email address entered above. To redirect other system roles' email to other accounts, use the same format.

- 5) Save the changes and then close the file.

- 6) Enter the following commands:

```
cf sendmail rebuild
```

```
cf daemon restart agent=sendmail
```

This rebuilds the configuration and database files, and restarts the sendmail servers.

Result

System email messages will now be sent to the aliased account instead of accumulating on the firewall's hard drive.

View administrator email messages

By default, a root alias is created for the administrator you set up when you configured your system. This alias automatically redirects system messages addressed to root to that first administrator's firewall-hosted account.

A mailbox is created the first time an administrator sends or receives an email message. Mailboxes for firewall administrators are stored in the */var/mail* directory.



Note: Do not ignore the email that accumulates on the firewall as it contains important information about your network and the firewall, and also uses disk space. Routinely read and delete email sent to the firewall, or have it redirected elsewhere.

To view system messages sent to firewall-hosted accounts, follow the steps below.

Steps

- 1) At a firewall command prompt, enter the following command to change to the Admn role:
`srole`
- 2) View email messages by entering one of the following:
 - `mail` — Displays your messages(messages for the logged-in administrator)
 - `mail -f root` — Displays messages addressed to root
 - `mail -f username` — Displays messages addressed to an administrator(*/var/mail* directory)



Tip: Refer to the `mail` man page for detailed information on using the `mail` command. If you prefer, you might use an alternate email program.

Result

Remember to check email frequently, particularly if you have attack and system event responses sent to *root*.

Related tasks

[Set up email aliases for administrator accounts](#) on page 506

VPN (virtual private networks)

Contents

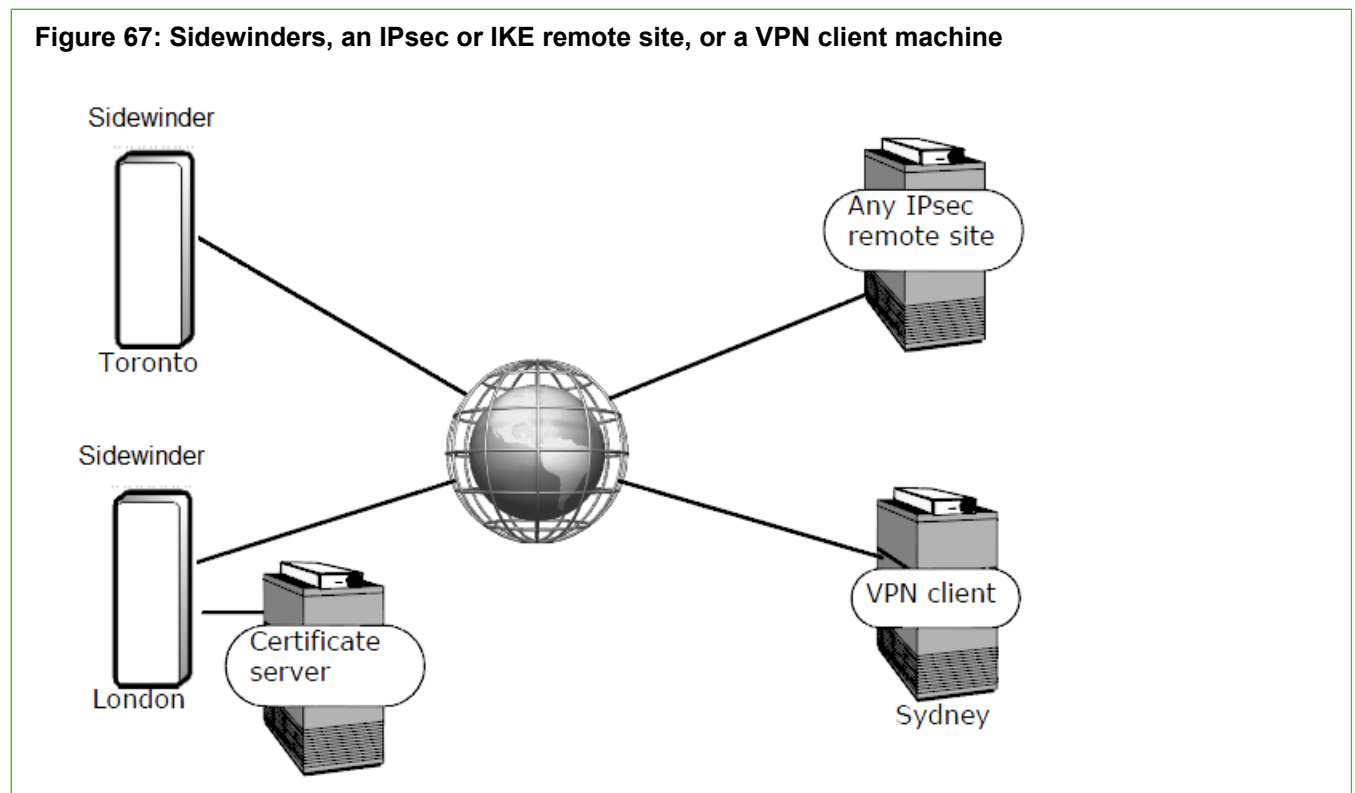
- [Benefits of the Sidewinder VPN solution](#) on page 509
- [Plan your VPN](#) on page 511
- [What VPN user interfaces help to do](#) on page 520
- [Example VPN Scenarios](#) on page 522
- [Create VPN policy](#) on page 532

The Sidewinder VPN solution provides secure data transmission across unsecured networks through an encryption and decryption process. The firewall uses the IPsec protocol suite to support this process.

Benefits of the Sidewinder VPN solution

The Sidewinder VPN solution is embedded in the architecture, making it an operating characteristic of the OS. This integration not only lets you apply access control rules to VPNs in the same way you do for physically connected networks, but also means that you use the Sidewinder VPN solution to coordinate corporate-wide network security policies.

Figure 67: Sidewinders, an IPsec or IKE remote site, or a VPN client machine



As companies expand to new locations and employees spend more time working out of the office, VPN solutions are becoming more important to businesses. Consider the value of encrypting and authenticating data in these situations:

- Passing traffic from firewall to firewall between offices located in different cities (gateway-to-gateway VPN)
- Passing traffic from employees working remotely to your network (client-to-gateway VPN)

Information protection

The Internet is a broadcast medium that is used to send information. While information is in transit, anyone can choose to monitor or intercept this information.

Sending information beyond your firewall via the Internet is like sending an unsealed envelope of important information via a courier service: you must trust that the courier will not read or steal the information.

To address this danger, the IETF (Internet Engineering Task Force) developed a standard for protecting data on unprotected (or untrusted) networks such as the Internet. The standard has become known as *IPsec*, meaning Internet-Protocol Security. In brief, IPsec calls for encrypting the data before it leaves the local host, then decrypting it when it is received at the destination or remote host. Once it is decrypted, the data assumes its original form and can be read as intended. No matter how long or circuitous its route through the Internet, the data remains private by virtue of this encryption.

What are encryption and authentication?

The two main components of IPsec security are *encryption* and *authentication*.

- **Encryption** — Encryption is the means by which plain text is translated into encrypted text. It ensures that the transmitted data remains private and unreadable until properly decrypted. Sidewinder uses an encryption key to encipher and decipher each unit of data sent between your site and the “partner” or remote VPN site.
- **Authentication** — VPN authentication prevents unauthorized individuals from tampering with the contents of the data being transmitted. It also prevents them from creating messages that claim to come from a particular place but are actually sent from somewhere else (such as the hacker’s home computer). Authentication is accomplished through two methods:
 - Data-integrity checking, which allows the receiver to verify whether the data was modified or corrupted during transmission.
 - Sender identification, which allows the receiver to verify whether the data transmission originated from the source that claims to have sent it.

When used together, encryption and authentication are very much like writing an encoded message, sealing it in an envelope, and then signing your name across the flap. The receiver can first verify that the signature is yours as a means of determining the origin of the message. Next, the receiver can determine if the contents have been viewed or altered by checking that the envelope seal has not been compromised. Once the receiver is assured of the authenticity of the message, they can decode the contents and know that the contents are as intended.

Related concepts

[IPsec keys and how they work](#) on page 511

IPsec keys and how they work

A key is a number that is used to electronically sign, encrypt, and authenticate data when you send it, and to decrypt and authenticate your data when it is received. When a VPN is established between two sites, two keys are generated for each remote end: an encryption key and an authentication key.

To prevent these keys from being guessed or calculated by a third party, a key is a large number. Encryption and authentication (or session) keys are unique to each VPN definition you create.

Once generated, these keys are exchanged (either automatically or manually) between the sites, so that each end of the VPN knows the other end's keys.

Firewall gives you two options to generate key pairs.

- **Manual key generation** — If the remote site is not Internet Key Exchange (IKE)-compliant, you might want to choose the manual method of key generation. With this method, the firewall provides randomly generated encryption and authentication keys (or you can create your own), which you must copy and pass to the remote end of the VPN via secure e-mail, diskette, or telephone. Repeat this process each time you generate keys. Manual keys are more labor intensive than automatic keys and rarely used.
- **Automatic key generation using IKE** — If the remote end of your VPN uses the IKE protocol, the firewall can manage the generation of session keys between sites automatically. This process also regularly changes the keys to avoid key-guessing attacks. Automatic keys are very common in today's network environments.

Plan your VPN

Before you create new VPN policy, plan the characteristics of the VPN based on your network environment, security requirements, authentication requirements, and the type of IPsec-compliant remote device to which the VPN will be established.

Understanding the options associated with each concept will assist you in creating your VPN definition. Study the following information to help you determine which VPN configuration best suits your network environment.

Use the following sections to plan your VPN:

Related concepts

[Order of VPN definitions](#) on page 518

[Choosing the appropriate VPN attributes](#) on page 511

[Choosing the appropriate authentication type](#) on page 515

[Virtual zones and how to restrict VPN access](#) on page 518

Choosing the appropriate VPN attributes

Use the following sections to determine the attributes for your VPN.

Determining the VPN mode

Creating a VPN involves establishing an association (or a trust relationship) between your Sidewinder and an IPsec-compliant remote firewall, host, or client. These devices are referred to as *VPN peers*.

The type of VPN peer you are working with determines the type of VPN you will create and the associated VPN mode for that peer. There are two types of VPN peers:

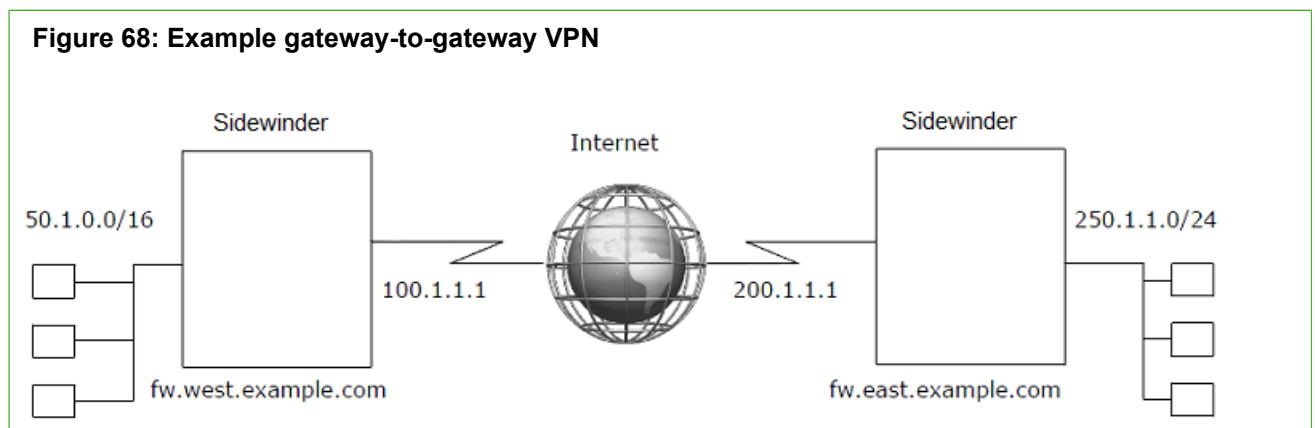
- **VPN gateways** provide encryption services to hosts on a set of protected networks behind the VPN gateway. Your Sidewinder functions as a VPN gateway. For example, VPN concentrators, home cable routers, and other firewall products with IPsec functionality. The following VPN modes are available for this VPN peer:

Table 88: Choosing VPN mode

If...	then the VPN type is	and the available modes are
The VPN peer has a dynamic IP address and will provide VPN access to clients that are behind it	Dynamic gateway-to-gateway	Dynamic IP Restricted Client
The VPN peer has a static IP address and will provide VPN access to clients that are behind it	Fixed gateway-to-gateway	Fixed IP
The VPN peer does not support IKE	Manual gateway-to-gateway	Manually Keyed VPN

For gateway-to-gateway VPNs, a VPN tunnel is established between the gateways to allow hosts behind them to communicate with each other.

Figure 68: Example gateway-to-gateway VPN



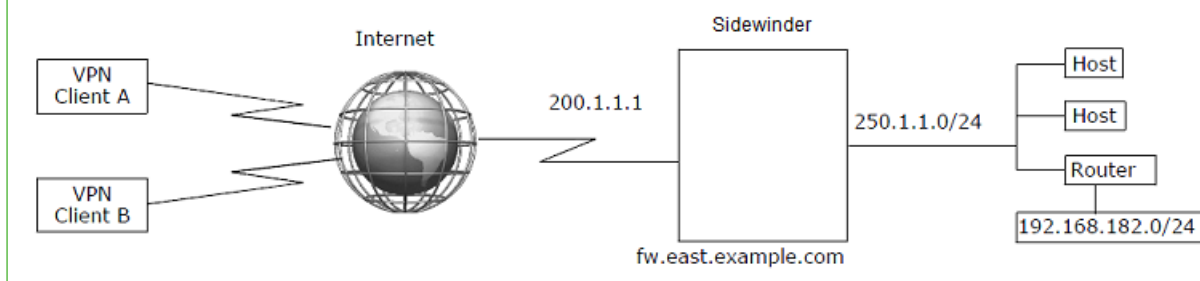
In the example above, the VPN tunnel is established between the firewalls, allowing the hosts in the 50.1.0.0/16 and the 250.1.1.0/24 networks to communicate securely.

- **VPN clients** provide encryption services to the host machine running the VPN client software. Typically, the VPN client software is installed on a remote user's laptop or mobile device and provides a secure connection between the laptop and a VPN gateway. The following VPN modes are available for this VPN peer:

Table 89: Choosing VPN mode

If...	then the VPN type is	and the available modes are
Multiple roving clients need VPN access	Dynamic client-to-gateway	<ul style="list-style-type: none"> • Dynamic IP Client • Dynamic IP Restricted Client

For client-to-gateway VPNs, the client(s) establish a VPN tunnel to the gateway to securely communicate with hosts behind the gateway.

Figure 69: Example client-to-gateway VPN

In this example, a VPN tunnel is established between each VPN client and the firewall, allowing the clients to communicate with the 250.1.1.0/24 network securely.

More about VPN modes:

- **Fixed IP** — Select this option if the IP address of the remote end is always the same. You must also provide the IP address of the remote end in the Remote IP field.
- **Dynamic IP Client** — Select this option if the remote end is a device whose IP address is not fixed. *Example: A traveling executive that gains Internet access from a laptop.*
- **Dynamic IP Restricted Client** — Select this option for client-to-gateway VPNs and dynamic gateway-to-gateway VPNs.
 - Client-to-gateway VPNs — Select this option to dynamically or statically assign a specific virtual address to each client. Assign a virtual address to the VPN clients to set up routing specific to remote VPN users. For the dynamic IP client mode, the public address of the laptop must be used.
 - If the remote peer is a gateway with a dynamic IP address, the dynamic virtual address range represents the real network that is behind the remote gateway.
 - If the remote peer is an individual client, the dynamic virtual address range represents the virtual IP address the client is configured to use.
 - Dynamic gateway-to-gateway VPNs — Select this option to define the protected network behind the dynamic gateway.
- **Bypass** — Select this option if you want certain traffic to bypass IPsec policy evaluation and be sent outside the encrypted tunnel. Other access control rules will apply to this traffic.
- **Manually Keyed VPN** — Select this option if you want to exchange session keys manually (for example, over the phone). You configure specific properties of the manual key exchange on the **Crypto** tab.



Note: This mode is most often used to provide compatibility with remote peers that do not support the Internet Key Exchange (IKE) protocol.

Related tasks

[Configure VPN definitions](#) on page 535

Differences between IKE versions

IKEv1 and IKEv2 are both available options on Sidewinder.

Some differences to note about the two versions:

- IKEv2 is simpler, more robust, and more reliable. However, not many products currently support the newer IKEv2. Check your product documentation.
- IKEv1 is not compatible with IKEv2. Both sides of a VPN connection must use the same version of IKE.

- When using IKEv2, each side of a VPN connection can use a different authentication method. With IKEv1, both sides must agree on an authentication method.
- In IKEv2, extended authentication (XAUTH) can be used as a standalone authentication method. In IKEv1, extended authentication must be used in conjunction with password/certificate authentication.

Determining if you will use IPv4 or IPv6 addresses

A VPN definition can use either IPv4 or IPv6 addresses, but not both.

For example, an IPv4-to-IPv6 VPN connection is not allowed. Both types of definitions can be used on the firewall at the same time.

Select IPv6 if you want a gateway-to-gateway connection between two IPv6 networks. The following restrictions apply to IPv6 addresses in a VPN definition:

- IPv6 must be enabled on the firewall.
- Only gateway-to-gateway VPNs can use IPv6 addresses.
- Client address pools are not allowed in definitions that use IPv6 addresses.
- Extended authentication is not allowed in definitions that use IPv6 addresses.
- NAT-T is not allowed in definitions that use IPv6 addresses.

Determining the encapsulation method

There are two methods for encapsulating packets in a VPN connection: transport mode and tunnel mode.

- **Transport mode** — In transport mode, only the data portion of the packet gets encrypted. This means that if a packet is intercepted, a hacker will not be able to read your information, but will be able to determine where it is going and where it has originated. This mode existed before firewalls and was designed for host-to-host communications.
- **Tunnel mode** — In tunnel mode, both the header information and the data is encrypted and a new packet header is attached. The encryption and new packet header act as a secure cloak or “tunnel” for the data inside. If the packet is intercepted, a hacker will not be able to determine any information about the true origin, final destination, or data contained within the packet because the packet header is encrypted. This mode is designed to address the needs of hosts that exist behind the firewall.

Benefits of using a client address pool

Client address pools are used to simplify the management of VPN clients by allowing the firewall to assign information to the client.



Note: Client address pools can only be used with VPN definitions using **Dynamic IP Restricted Client** mode.

- An IP address for the client's virtual network adapter
- DNS servers that are available to the client
- WINS servers that are available to the client

All the client needs is:

- Client software that supports ISAKMP Mode Configuration (IKEv1) or Configuration Payload (IKEv2) exchange
- Authorization information (a client certificate, a password, etc.)
- The address of the firewall

For a client address pool, an administrator creates a range or a 'pool' of IP addresses that will be used by remote peers when they attempt to make a VPN connection. When a client attempts a connection, the firewall assigns it one of the IP addresses available in the address pool. The firewall also negotiates with the client to determine other VPN requirements, such as which DNS and/or WINS servers will be made available to the client. If the negotiation is successful, the client is connected and the VPN connection is established.



Note: Not all VPN client software supports the negotiation of every client address pool parameter. Be sure to verify that your client(s) support the necessary features.

You define the number of IP addresses available in the client address pool. Even though the client might have a fixed IP address, the address used within the VPN definition is the address assigned to it from the address pool. The address pool works for both fixed and dynamic clients. Refer to the VPN scenarios where address pools could be used:

You can also create multiple client address pools. Grouping VPN clients into distinct pools allows you to limit the resources the clients in each group can access.

Related reference

[Scenario 2: Simple deployment of remote users](#) on page 524

[Scenario 3: Large scale deployment of clients](#) on page 528

Choosing the appropriate authentication type

Use the following sections to determine which authentication method(s) are appropriate for your VPN.

Related concepts

[IKE VPN authentication techniques](#) on page 515

[Guidelines for selecting a VPN authentication type](#) on page 516

Related tasks

[Configure certificate or CA information](#) on page 535

IKE VPN authentication techniques

When using automatic key generation, after you gather the initial information for the remote end of the VPN, there is no further direct contact between you and the remote end of the VPN.

Session keys are automatically and continually generated and updated based on this initial identifying information. As a result, the firewall requires a way to assure that the machine with which you are negotiating session keys is actually who they claim to be—a way to authenticate the other end of the VPN. To allow automatic key generation, the firewall offers the following authentication techniques:



Note: If you are using manual key generation, each time you generate session keys you must communicate directly with the other end of the VPN via telephone, diskette, or e-mail. By

contacting the remote end of the VPN each time you change session keys, you manually verify that the remote end is actually who they claim to be.

- **Pre-shared password** — The firewall and the remote end must both use the agreed-upon password, defined during the initial configuration of the VPN, to authenticate each other.
- **Single certificate** — Single certificate authentication requires that the firewall generate a certificate and private key to be kept on the firewall and a certificate and private key to be exported and installed the peer. Each certificate, once installed on its end of a VPN connection, acts as a trust point. A single certificate (also referred to as a “self-signed certificate”) differs from certificate authority (CA) based certificates in that no root certificate is necessary.
- **Certificate Authority policy** — The firewall can be configured to trust certificates from a particular certificate authority (CA). The firewall will trust any certificate that is signed by the chosen CA and meets certain administrator-configured requirements on the identity contained within the certificate. We recommend that only locally administered certificate authorities be used in this type of policy.
- **Extended authentication (XAUTH)** — The extended authentication (XAUTH) option requires the person requesting the remote access VPN connection to validate their identity. The extended authentication option is most useful if you have traveling employees that connect remotely to your network using laptop computers. If a laptop computer is stolen, without extended authentication it might be possible for an outsider to illegally access your network, since the information needed to establish the VPN connection (the self-signed certificate, etc.) is saved within the VPN client software. When extended authentication is used, however, a connection will not be established until the user enters an additional piece of authentication information that is not saved on the computer—either a one-time password, passcode, or PIN. This additional level of authentication renders the VPN capabilities of the laptop useless when in the hands of a thief.

More notes regarding authentication using IKE:

- If using IKEv1, both sides of a VPN connection must use the same version of IKE and the same authentication method
- If using IKEv2, each side of a VPN connection can use a different authentication method
- If using IKEv1, XAUTH is used in conjunction with Password, Certificate and Certificate Authority, and Single Certificate
- If using IKEv2, XAUTH is used as the sole authentication method

If you are using automatic key generation and intend to use certificates for authentication, you should configure the certificate and/or Certificate Authority (CA) server information before you set up the VPN. This eliminates the need to configure certificates and CAs during the VPN process.

Related concepts

[Why use certificates](#) on page 617

Guidelines for selecting a VPN authentication type

The type of authentication for a VPN is dependent on the type of VPN peer as well as the VPN mode.



Note: Extended authentication is available only for dynamic client-to-firewall configurations.

Table 90: VPN authentication options

If the VPN type is	the available VPN modes are	and the Authentication options are
Dynamic gateway-to-gateway	<ul style="list-style-type: none"> Dynamic IP Restricted Client 	<ul style="list-style-type: none"> Automatic key shared password VPN Automatic key single certificate VPN Automatic key certificate authority-based VPN
Fixed gateway-to-gateway	<ul style="list-style-type: none"> Fixed IP 	<ul style="list-style-type: none"> Automatic key shared password VPN Automatic key single certificate VPN Automatic key certificate authority-based VPN
Client-to-gateway	<ul style="list-style-type: none"> Dynamic IP Client Dynamic IP Restricted Client 	<ul style="list-style-type: none"> Automatic key shared password VPN Automatic key single certificate VPN Automatic key certificate authority-based VPN Extended authentication (XAUTH)
Manual gateway-to-gateway	<ul style="list-style-type: none"> Manually Keyed VPN 	<ul style="list-style-type: none"> Manual key VPN

Follow these general guidelines when deciding which type of VPN to use:

- For a small number of VPN peer clients with dynamically assigned IP addresses, the single certificate VPN is a cost-effective solution. A shared password VPN in conjunction with extended authentication is also an option.
- If the VPN peer has a static IP address, the pre-shared password VPN is the easiest to configure. Extended Authentication would not be used in a gateway to gateway configuration as there is no one to provide the challenge/response.
- If there is a large number of VPN peer clients with dynamically assigned IP addresses (such as a traveling sales force), the CA-based VPN is often the easiest to configure and maintain. Another popular option is to use a pre-shared password VPN in conjunction with extended authentication.
- If the VPN peer is not a Forcepoint product, and all other types of VPN methods do not work, try the manual key VPN.

Order of VPN definitions

The order of definitions in the **VPN Definitions** window affects how packets are matched to definitions. The first definition that matches a connection request is used to allow or deny that connection.

For example, the table below shows the first two positions in a list of VPN definitions. If a packet has a source IP address of 10.69.106.5 and a destination IP address of 10.69.104.20, it is matched to the first definition in the list. The search is stopped before the packet is compared to the more precise match in the second definition.

Table 91: VPN definition ordering

Position	Local Network	Remote Network
1	10.69.106.0/24	10.69.104.0/24
2	10.69.106.5/32	10.69.104.20/32

You can also select certain traffic to bypass IPsec policy evaluation and be sent outside the encrypted tunnel. Other access control rules will apply to this traffic. You select this option on the **VPN Definitions: General** tab.

Example: Traffic between two networks at two different sites is encrypted, but you want traffic to and from the web server to be sent outside the encrypted tunnel. You would configure a Bypass definition and place it in front of a more general definition in the **VPN Definitions** list.

The table below shows a **VPN Definitions** list with a Bypass VPN definition in the first position.

Table 92: Bypass definition in the VPN Definitions list

Position	Action	Local Network	Remote Network
1	Bypass	10.69.106.0/24	10.69.104.20/32
2	IPsec	10.69.106.0/24	10.69.104.0/24

Virtual zones and how to restrict VPN access

You can familiarize yourself with virtual zone concepts and to determine if you should use a virtual zone to restrict the access allowed by your VPN.

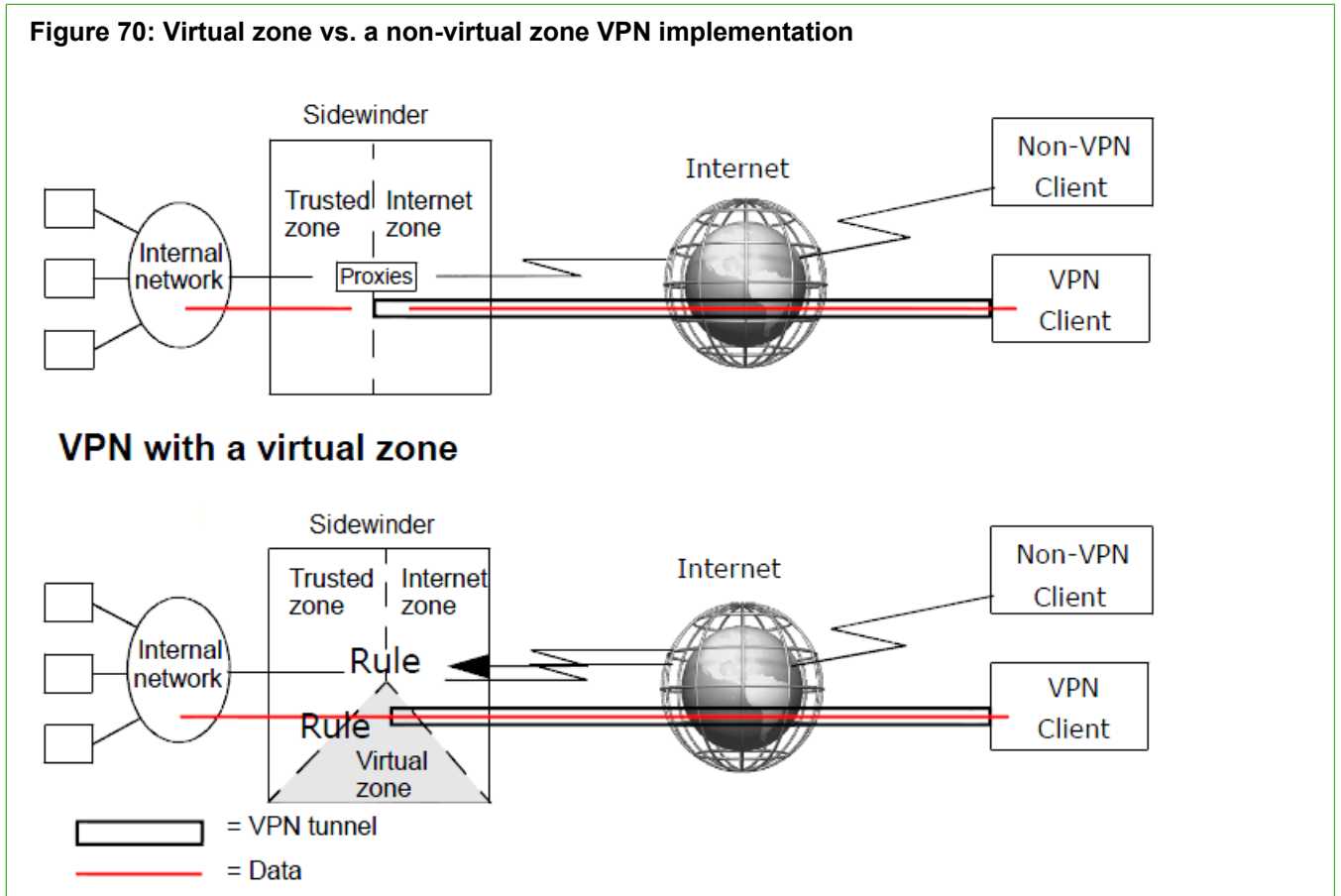
Virtual zones and how to implement them

A termination zone is the zone in which VPN traffic transitions between plain-text and encrypted data. You can increase security and control of that transition by using a virtual zone as your termination zone.

A virtual zone is a zone that does not contain a network interface card (NIC). VPNs terminated in a virtual zone require access control rules to take traffic from the virtual zone to and from the internal zone. Using a virtual zone separates VPN traffic from non-VPN traffic, and it allows you to enforce a security policy that applies strictly to your VPN users.

Consider a VPN policy that is implemented without the use of a virtual zone. Not only will VPN traffic mix with non-VPN traffic, but there is no way to enforce a different set of access control rules for the VPN traffic. This is because rules are applied on a zone basis, not to specific traffic within a zone. By terminating the VPN in a virtual zone, you effectively isolate the VPN traffic from non-VPN traffic. In addition, you are able to configure a unique set of access control rules for the virtual zone that allows you to control precisely what your VPN users can or cannot do. Figure 27-108 illustrates this concept. See the illustration below.

Figure 70: Virtual zone vs. a non-virtual zone VPN implementation



- Traffic originating from the remote peer must now use an access control rule to move from the virtual zone to the internal zone.
- A separate access control rule is used for traffic originating from the internal network destined for the remote peer.

Once the traffic is decrypted on the firewall, it also needs an access control rule configured for traffic from the virtual zone to the internal zone. This allows administrators to have a finer grain of control of the services allowed inbound and outbound from their controlled networks.

You can define up to 63 physical and virtual zones. For example, if you have two distinct types of VPN definitions and you want to apply a different set of access control rules to each type, create two virtual zones, then configure the required access control rules for each virtual zone.

One question that might come to mind when using a virtual zone is: “How does VPN traffic get to the virtual zone if it doesn’t have a network card?” All VPN traffic originating from the Internet initially arrives via the network interface card in the Internet zone. A VPN connection, however, can internally route and logically terminate VPN traffic in any zone on the firewall. By defining a VPN connection to terminate the VPN in a virtual zone, the VPN traffic is automatically routed to that virtual zone within the firewall. Thus, the trusted network now recognizes the virtual zone as the source zone for your VPN traffic. From the virtual zone, an access control rule is needed to move the traffic to a trusted zone with network access.

Related tasks

[Create and use a virtual zone with a VPN](#) on page 534

Benefits of using access control rules to direct VPN traffic

You can use VPN definitions in conjunction with access control rules to gain more control over your network security policy.

There are several advantages to using access control rules to restrict traffic bound for a VPN, including:

- You can control which services are allowed through the VPN by filtering traffic based on protocol and port.
- Rule-level auditing of inbound/outbound connections is included. Since the VPN audit only indicates when the encrypted connection is established or torn down, access control rules can provide the added benefit of auditing for each connection between a VPN's protected hosts.
- Traffic can be inspected for malicious content by applying application defenses to the access control rules. All features of the firewall rules can be used to protect internal resources and monitor what external resources are being used.
- You use access control rules to restrict access at the user level, such as per-user authentication.
- NAT and redirection are not recommended in access control rules controlling VPN traffic. If your environment requires the use of NAT and redirection, see Knowledge Base article [9287](#).

What VPN user interfaces help to do

The following sections describe some of the VPN user interfaces.

Related concepts

[What the ISAKMP server does](#) on page 522

Related reference

[What you can define on the VPN Properties window](#) on page 520

[What you can define on the Client Address Pools window](#) on page 521

What you can define on the VPN Properties window

The **VPN Properties** window contains several tabs for configuring a VPN.

- **General** — Provide basic information about the VPN definition.
- **Remote Authentication** — Define the authentication method that will be used by the remote peer in this VPN definition. You can also define the characteristics of the selected authentication method.



Note: Authenticating the remote peer prevents access to the VPN from Internet hosts masquerading as the remote peer.

- **Local Authentication** — Define the authentication method that will be used by the firewall in this VPN definition. You can also define the characteristics of the selected authentication method. Select one of the following options:

- **Password** — Select this method to authenticate to the remote peer using a password.
- **Certificate** — Select this method to authenticate to the remote peer using a certificate.
- **Crypto** — Define the IPsec cryptographic properties according to the type of key exchange:
 - Manual key exchange — Define manual authentication for this VPN definition.
 - Automatic key exchange — Define the IPsec cryptographic and hashing algorithms used to in this VPN definition.
- **Advanced** — Define some of the more advanced points of a VPN definition on this tab, including NAT Traversal. Only administrators that are highly schooled in VPN should modify the information on this tab. This information is used only with automatic key exchange.

Related tasks

[Configure the General tab](#) on page 539

[Configure the Remote Authentication tab](#) on page 541

[Configure the Local Authentication tab](#) on page 545

[Configure the Crypto tab](#) on page 546

[Configure the Advanced tab](#) on page 548

What you can define on the Client Address Pools window

The **Client Address** window contains the several tabs.

- **Subnets** — Define the virtual and local subnets
- **Servers** — Define the DNS server(s) and/or the WINS server(s)
 - These servers provide name and address resolution services for devices within the local network.
 - The DNS servers you specify can reside on the firewall or be located on another machine in a local or remote network.
 - WINS servers are never located on the firewall.
- **Fixed IP Map** — Define fixed addresses for selected clients
 - It enables each of the specified clients to connect to the firewall using its own unique IP address.
 - It effectively reserves a specific IP address for a specified client.
 - The fixed addresses you specify must be within the range of available IP address as defined by the client address pools.

One of the benefits of assigning fixed IP addresses to selected clients is that it allows you to govern what each client can do. For example, you might restrict access to certain clients, and you might grant additional privileges to other clients. You do this by creating a network object for a selected IP address and then using the network object within an access control rule.

The **Fixed IP Map** tab contains a **Fixed IP Client Address Mappings** box that lists the current IP address/client mappings. Each unique IP address can appear in the table only once. Multiple identities representing a single client, however, can be mapped to one IP address.

Related tasks

[Configure the Subnets tab](#) on page 551

[Configure the Servers tab](#) on page 553

[Manage the fixed IP map](#) on page 556

What the ISAKMP server does

Sidewinder uses the ISAKMP server to generate and exchange keys for VPN sessions. The ISAKMP server properties includes audit, negotiation and connection, and extended authentication parameters.

Related tasks

[Configure the ISAKMP server](#) on page 557

Example VPN Scenarios

The following sections describe three typical VPN scenarios.

Each scenario begins by describing a particular VPN requirement. It then explains how to implement the solution using the Admin Console. These scenarios assume that the proper access control rule(s) are defined to allow ISAKMP traffic on the proper zone(s). In the scenarios that follow it is assumed an access control rule has been defined that allows ISAKMP traffic on the Internet zone.



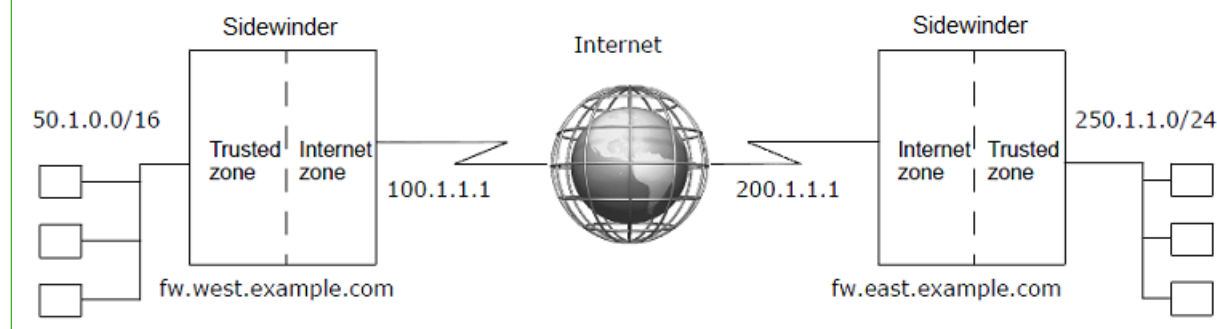
Note: The values used in the following scenarios are for demonstration purposes only.

Scenario 1: Firewall-to-firewall VPN using a shared password

The easiest type of VPN definition to configure is one that uses a shared password for authentication.

A shared password is typically used to establish a VPN connection between two corporate offices that have static IP addresses. Such a situation occurs if you have a business partner that requires access to your network, or if you have one or more corporate divisions located in different cities.

The following figure provides the sample configuration information used in this scenario.

Figure 71: VPN between two corporate offices

Requirements

This VPN scenario requires the following.

- A VPN connection between two corporate offices
- Shared password authentication
- Static IP addresses for each peer in the VPN definition

Implementation

The following steps show the fields on the VPN menus that must be defined to create this VPN definition. The configuration steps are performed on the firewall named fw.east.example.com.

Select **Network > VPN Configuration > VPN Definitions**, and then click **New**. The **VPN Properties** window appears.

1) On the **General** tab, enter the following details.

- **Name** — corporate_west
- **Enabled** — Yes
- **Mode** — Fixed IP
- **Client Address Pool** — <disabled>
- **IKE Version** — V1
- **Zone** — Trusted
- **Encapsulation** — Tunnel
- **Local IP** — localhost
- **Local Network / IP** — 250.1.1.0/24
- **Remote IP** — 100.1.1.1
- **Remote Network / IP** — 50.1.0.0/16



Note: When configuring the firewall named fw.west.example.com, the Local Network/IP and the Remote Network/IP values are reversed and the Remote IP value is 200.1.1.1.

2) On the **Remote Authentication** tab:

- **Remote Authentication Method** — password
- **Enter Remote Password** — samplepassword

- **Verify Remote Password** — samplepassword
 - **Remote Identity** — Gateway IP Address (100.1.1.1)
- 3) On the **Local Authentication** tab:
 - **Local Authentication Method** — password (not editable)
 - **Enter Local Password** — samplepassword (not editable)
 - **Verify Local Password** — samplepassword (not editable)
 - **Local Identity Type** — IP Address
 - **Value** — localhost
 - 4) On the **Crypto** tab: Select the algorithms to match the other firewall.
 - 5) On the **Advanced** tab: No changes needed.
 - 6) Click **Add** to save the new VPN definition.
 - 7) Save your changes.

VPN Scenario 1 Summary

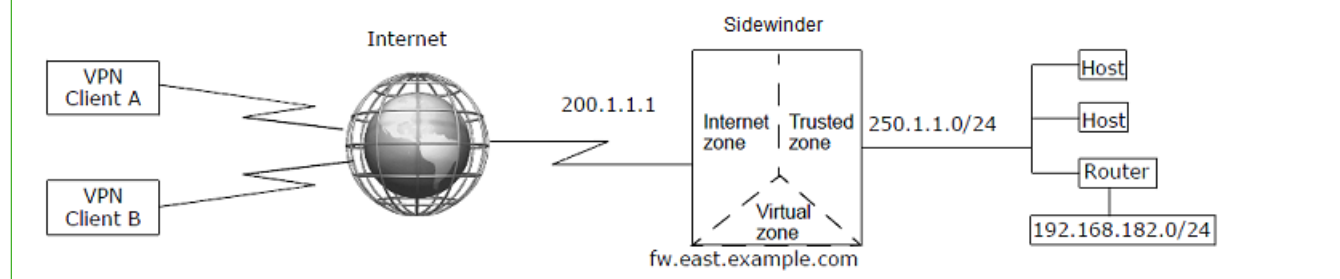
The VPN can be used as soon as you configure the other firewall. Enter the same type of information, changing the IP addresses as appropriate.

Scenario 2: Simple deployment of remote users

A common reason for using a VPN is to allow your travelling employees to connect to your corporate network from a remote site.

This connection is typically made between an employee's laptop computer and your corporate Sidewinder. In this type of VPN definition, single (also known as "self-signed") certificates are generated by the firewall and distributed to each remote peer. This type of VPN can be used with dynamic IP-assigned clients and gateways. Create one definition for each client, so this type of VPN is typically used only if you have a small number of remote peers.

The figure below provides the sample configuration information used in this scenario. Note that the remote end of this VPN connection (from the firewall point of view) is a laptop that will be using a dynamic IP address.

Figure 72: One VPN definition per client

Assumptions

The VPN scenario assumes the following:

- A VPN connection between a remote computer and the firewall
- A self-signed firewall certificate that is generated by the firewall
- One or more remote certificates that is generated by the firewall and distributed to the remote peers
- One VPN definition per remote peer
- Each VPN definition is terminated in the Virtual zone
- VPN clients should have access to the 250.1.1.0 network but not the 192.168.182.0 network
- All clients make connections using a virtual IP address assigned from a client address pool
- All clients use VPN client software that supports mode-config



Note: When determining your deployment method, consider what steps you will take to ensure the protection of your private key material. Allowing unauthorized access to your private key material could compromise your entire network.

Implementation

These steps show the fields on the VPN menus that must be defined in order to create this VPN definition.

- 1) Create and export a firewall certificate:
 - a) In the Admin Console, select **Maintenance > Certificate/Key Management**.
 - b) On the **Firewall Certificates** tab, click **New** and create a firewall certificate by specifying the following:
 - **Certificate Name** — MyFirewall_cert
 - **Distinguished Name** — CN=MyFirewall,O=bizco,C=US
 - **Key type** — RSA
 - **Key length** — 2048
 - **Digest** — SHA1
 - **Submit to CA** — Self Signed
 - Click **Add**, then click **Save**.
 - c) [Optional] On the **Firewall Certificates** tab, click **Export** and export the firewall certificate by specifying the following:
 - Select **Export Firewall Certificate to File**

- Click **Browse** and specify where you want to save the firewall certificate. The firewall certificate is often saved to an accessible location (portable storage device or protected network) for distribution to the client.
 - Click **OK**.
- 2) Create a remote certificate for each client:
- a) On the **Remote Certificates** tab click **New** and create a self-signed certificate for a client by specify the following:
 - **Certificate Name** — Sales_A
 - **Distinguished Name** — CN=Sales_A,O=bizco,C=US
 - **Key type** — RSA
 - **Key length** — 2048
 - **Digest** — SHA1
 - **Submit to CA** — Self Signed
 - Click **Add**.
 - Click the **Save** icon.
 - b) Repeat Step a for each remote peer.
 - c) On the **Remote Certificates** tab, click **Export** and export the remote certificate by specifying the following:
 - Select **Export Certificate and Private Key**.
 - Select **Export Certificate/Key As One File**.
 - Export Client Private Key to File: Click **Browse** and specify where you want to save the private key.
 - Click **OK**.
 - d) Repeat Step c for each remote peer. When you are finished you should have the public firewall certificate as well as either the PKCS12-formatted object or the certificate/key file pair for that client saved to a location accessible by the remote peer (portable storage device or network).

3) Create a client address pool.

Using a client address pool lets you define which local networks the clients can access. For this example, assume you want to permit access to the 250.1.1.0 network but not the 192.168.182 network.



Note: Your client software must support this capability.

- In the Admin Console, select **Network > VPN Configuration > Client Address Pools**, and then click **New**. The **Pool Entry** window appears.
- **Enter New Pool Name** — SalesPool
- **Virtual Subnet** — 10.1.1.32/27
- Click **New**. In the **Local Subnet** field, enter 250.1.1.0/24 and then click **Add**.
- Click **Add** to add the new pool.



Note: The **Subnet** and **Number of Bits in Netmask** fields work in concert to determine the network portion of the addresses in the pool as well as the total number of addresses in the pool. The values shown here provide 30 possible addresses: 10.1.1.33 - 10.1.1.62.

Modify these two values as appropriate for your situation. (For example, in this scenario you might alternatively specify IP Address = 10.1.1.16 and Netmask = 28, creating 14 possible addresses: 10.1.1.17 - 10.1.1.30.)

- On the **Servers** tab: If the client software you are using supports this mode-config capability, specify your internal DNS and WINS servers here.
 - Click **Add**.
- 4) Create a VPN definition for each client:
- a) Select **Network > VPN Configuration > VPN Definitions**, and then click **New** to configure a new definition. The **VPN Properties** window appears.
 - b) On the **General** tab:
 - **Name** — Sales_A
 - **Enabled** — Yes
 - **Mode** — Dynamic IP Restricted Client
 - **Client Address Pool** — SalesPool
 - **Zone** — Virtual
 - **Encapsulation** — Tunnel
 - **Local IP** — localhost
 - c) On the **Remote Authentication** tab:
 - **Remote authentication method** — Single Certificate
 - **Remote Certificate** — Select the certificate you created in step 1C for this client
 - d) On the **Local Authentication** tab:
 - **Local authentication method** — Single Certificate (not editable)
 - **Firewall Certificate** — Select the certificate you created in step 1A
 - e) On the **Crypto** tab: No changes needed.
 - f) On the **Advanced** tab: [Conditional] If the clients are expected to be behind a NAT device, select **Enable NAT Traversal**.
 - g) Click **Add** to save the new VPN definition, then click **Save**.
- 5) Repeat Step 4 for each client, changing the name and the remote certificate as appropriate.

Summary

Each individual VPN connection can be used as soon as the remote peers are configured.

Each client needs the client-specific certificate and private key information you saved in Step 1 and Step 2 to configure their end of the VPN connection. If you saved this information to removable media you can either hand it to them in person, e-mail it to them, or perform the imports while the machine is within a trusted network. It is not safe to distribute certificate and private key information via e-mail.



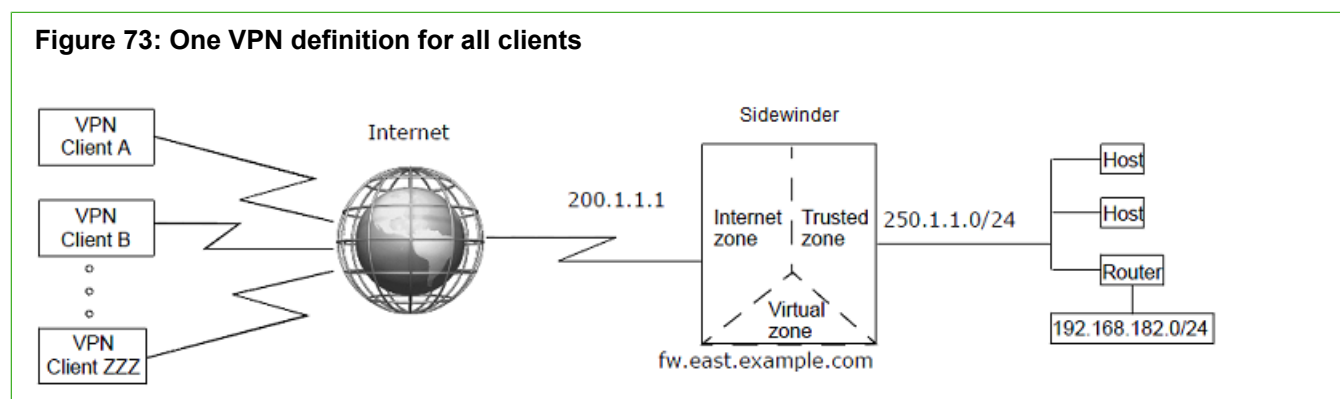
Note: The configuration described above restricts VPN traffic by terminating it in a virtual zone. Access control rules must be configured to specify what access the VPN clients have to the trusted network.

Scenario 3: Large scale deployment of clients

This scenario is similar to Scenario 2 except that instead of a small number of remote peers it assumes you have hundreds or even thousands of remote peers.

Because it is unreasonable to create a unique VPN definition for each client, a Certificate Authority (CA) will be used. The CA, in conjunction with the remote identities you define, allows you to create one VPN that is accessible by all of the clients.

The following figure provides the sample configuration information used in this scenario.



Assumptions

This VPN scenario assumes the following:

- A VPN connection between a Sidewinder and many clients
- A Certificate Authority-based VPN
- A single VPN definition for all clients with a like security policy rather than one definition per client
- The VPN connection is terminated in a virtual zone
- The clients can have dynamic or static IP addresses
- VPN clients should have access to the 250.1.1.0 network but not the 192.168.182.0 network
- All clients make connections using a virtual IP address assigned from a client address pool
- All clients are using VPN client software that supports mode-config




Note: It is assumed in this scenario that the clients do not have access to the CA and must rely on the firewall to create and distribute the necessary certificates and private keys.

Implementation

The following steps show the fields on the VPN menus that must be defined in order to create this VPN definition.

- 1) Define the CA used with this VPN:

- a) In the Admin Console, select **Maintenance > Certificate/Key Management**.
 - b) Click the **Certificate Authorities** tab.
 - c) Click **New** and create a CA by specifying the following:
 - **CA Name** — BizcoCA
 - **Type** — SCEP (or whatever value is appropriate)
 - **URL** — http://10.18.128.8
 - d) Click **Add**.
 - e) Click the **Save** icon to save your changes.
 - f) Click **Get CA Cert** (Retrieves the CA Cert from the URL address.)
 - g) Click **Get CRL** (Retrieves the **Certificate Revocation List** for this CA.)
- 2) Create a firewall certificate that is signed by the CA:
- a) Click the **Firewall Certificates** tab.
 - b) Click **New** and create a firewall certificate by specifying the following:
 - **Certificate Name** — BizcoFW_by_CA
 - **Distinguished Name** — CN=BizcoFW_by_CA,O=Bizco,C=US
 - **Key type** — RSA
 - **Key length** — 2048
 - **Digest** — SHA1
 - **Submit to CA** — BizcoCA
 - c) Click **Add**, then click **Save** to save your changes.
 At this point the **Status** field for this certificate will be `PENDING`. This is because the request has been sent to the CA but the certificate has yet to be created. The status will remain `PENDING` until the CA administrator approves your request.
 - d) Click **Query**. This queries the CA to see if the certificate is approved. If yes, the Status field will change to `SIGNED` and the certificate is imported.
-  **Note:** The firewall automatically queries the CA every 15 minutes to see if the request has been accepted. If the request has been accepted, the firewall will retrieve the resulting certificate.
- 3) Create one or more identities that define who is authorized to use this VPN:
- a) Click the **Remote Identities** tab.
 - b) Click **New** and create one or more identities that define who is authorized to use this VPN.
 - **Identity Name**— Sales_force

- **Distinguished Name** — CN=*,OU=sales,O=bizco,C=us
- c) Click **Add**.
 - d) Click **Close**, then click **Save** to save your changes.
- 4) Create a client address pool:
Using a client address pool lets you define which local networks the clients can access. For this example, assume you want to permit access to the 250.1.1.0 network but not the 192.168.182 network.



Note: Your client software must support this capability.

- a) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.
- b) Click **New** and create a new client address pool by specifying the following:
 - **Enter New Pool Name** — SalesPool
 - **Virtual Subnet** — 10.1.1.0/24
 - Click **New**. In the Local Subnet field, enter 250.1.1.0/24 and then click **Add**.
- c) Click **Add** to add the new pool.



Note: The **IP Address** and **Number of Bits in Netmask** fields work in concert to determine the network portion of the addresses in the pool as well as the total number of addresses in the pool. The values shown here provide 254 possible addresses: 10.1.1.0–10.1.1.255. Modify these two values as appropriate for your situation.

- d) If the client software you are using has mode-config capability, specify your internal DNS and WINS servers on the **Servers** tab.
 - e) Click the **Save** icon to save your changes.
- 5) Create the VPN definition:
- a) Select **Network > VPN Configuration > VPN Definitions**.
 - b) Click **New** to configure a new definition. The **VPN Properties** window appears.
 - c) On the **General** tab:
 - **Name** — Large_scale_sales
 - **Enabled** — Yes
 - **Mode** — Dynamic IP Restricted Client
 - **Client Address Pool** — VPNPool
 - **Zone** — Virtual
 - **Encapsulation** — Tunnel
 - **Local IP** — localhost

- d) On the **Remote Authentication** tab:
 - **Authentication method** — Certificate + Certificate Authority
 - **Certificate Authorities** — BizcoCA (created in step 1A)
 - **Remote Identities** — Sales_force (created in step 1C)
- e) On the **Local Authentication** tab:
 - **Authentication method**— Certificate (not editable)
 - **Firewall Certificate** — BizcoFW_by_CA (created in step 1B)
- f) On the **Crypto** tab: Order the algorithms to match that of the client.
- g) On the **Advanced** tab: [Conditional] If the clients are expected to be behind a NAT device, select **Enable NAT Traversal**.
- h) Click **Add** to save the new VPN definition, then click **Save** to save your changes.

6) Create the client certificates for each client:



Note: You can skip this step and Step 7 for those clients that have online access to the CA. These clients can create and retrieve their own certificates.

- a) In the Admin Console, **Maintenance > Certificate/Key Management**.
 - b) Click the **Remote Certificates** tab.
 - c) Click **New** and create a certificate for a client by specifying the following:
 - **Certificate Name** — Sales_A
 - **Distinguished Name** — CN=Sales_A,OU=sales,O=bizco,C=US
 - **Key Type** — RSA
 - **Key length** — 2048
 - **Digest** — SHA1
 - **Submit to CA** — BizcoCA
 - **Private Key** — Click **Browse** and specify where you want to save the private key associated with this certificate. In this scenario it is common to save the certificate to the same location as the exported firewall certificate.
 - **Certificate** — Click **Browse** and specify where you want to save this certificate. In this scenario it is common to save the certificate to the same location as the private key and the exported firewall certificate.
 - d) Click **Add**, then click **Save** to save your changes.
- 7) Provide certificate information and/or files to clients as necessary
- a) Select **Maintenance > Certificate/Key Management**. Export the CA certificate and the public firewall certificate to the same location used in Step 6.

- b) On the **Certificate Authorities** tab, select the CA certificate you created in Step 1, then click **Export** and export the certificate by specifying the following:
 - **Destination** — File
 - **Generated CA Certificate File** — Click **Browse** and specify where you want to save the CA certificate. Add the .pem extension to the file name.
 - Click **OK**.
 - c) [Optional] On the **Firewall Certificates** tab, select the firewall certificate you created in Step 2, then click **Export** and export the certificate by specifying the following:
 - **Destination** — File
 - **Export Firewall Certificate to File** — Click **Browse** and specify where you want to save the firewall certificate. Add the .pem extension to the file name.
 - Click **OK**.
- 8) Repeat Step 6 and Step 7 for each remote peer.
When you are finished your storage location should have four items for each remote peer: the CA certificate, the firewall certificate, the unique private key for the client, and the remote certificate public key for the client.

Summary

The firewall is ready to accept connections across this VPN as soon as the remote peers are configured.

To configure their end of the VPN connection, each client needs the client-specific certificate and private key information you saved in Step 6, the CA certificate you created in Step 1, and the firewall certificate you created in Step 2. If you saved this information to removable media you can either distribute the information in person or e-mail it to them, or perform the imports while the machine is within a trusted network. It is not safe to distribute certificate and private key information via e-mail.



Note: The configuration described above restricts VPN traffic by terminating the VPN connection in a virtual zone. Access control rules must be configured to specify what access the VPN clients have to the trusted network.

Create VPN policy

High level overview of the tasks required to create a Sidewinder VPN.



Note: Because the configuration possibilities are substantial, this section does not cover specifics. Before you use this section to create a new VPN, make sure you have planned your VPN configuration.

Follow these high level tasks to set up a VPN:

Steps

- 1) Plan the VPN implementation from end to end.

- 2) Configure the ISAKMP server.
 - a) Select **Network > VPN Configuration > ISAKMP Server**. The **ISAKMP Server** window appears.



Tip: For option descriptions, click **Help**.

- b) Configure the server options and the XAUTH method.
- 3) [Conditional] If you are creating a Dynamic IP Restricted Client VPN and want the firewall to assign resources to the remote peer, create a client address pool.
Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.

- 4) Define the VPN.
Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Note: If you want to restrict VPN traffic using a virtual zone, we recommend that you simplify the configuration process by first configuring a new VPN without a virtual zone. After you have verified that the VPN is working, you can then add a virtual zone to restrict access.

- 5) [Conditional] If you want to restrict VPN access using a virtual zone, create a virtual zone and terminate the VPN in that zone.
Select **Maintenance > Configuration Backup**. The **Configuration Backup** window appears.

Related concepts

[What VPN user interfaces help to do](#) on page 520

Related tasks

[Plan your VPN](#) on page 511

Set up the ISAKMP server

If you are using automatic key exchange, you must complete several steps before using any automatic key VPNs.

Steps

- 1) Configure the (Internet Security Association and Key Management Protocol) ISAKMP server.

- 2) Create an access control rule to allow access to the ISAKMP server:



Tip: For option descriptions, click **Help**.

Select **Policy > Access Control Rules**, then click **New** to create an access control rule for the ISAKMP server. The ISAKMP rule must contain the following values:

- **Application** — ISAKMP Server
- **Source Zone** — The zone receiving traffic from the VPN peer(s)
- **Source endpoint** — <Any> (or addresses of remote VPN peer(s))
- **Destination Zone** — Match the source zone setting

Related tasks

[Configure the ISAKMP server](#) on page 557

Create and use a virtual zone with a VPN

Using a virtual zone in your VPN allows you to enforce policy on the VPN traffic.

Steps

- 1) Create the virtual zone:
 - a) Select **Network > Zone Configuration**. The **Zone Configuration** window appears.
- 2) Save the changes.
- 3) Configure the access control rules.

Select **Policy > Access Control Rules** and define the rules that allow access to and from the virtual zone.



Note: The virtual zone should be specified as either the source or destination zone, depending on the type of access control rule being defined.

- 4) Terminate the desired VPN connection(s) in the virtual zone:
 - a) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.
 - b) From the **VPN definitions** list, select the VPN definition you want to terminate in the virtual zone.
 - c) From the **Zone** drop-down list, select the virtual zone that you created.

- d) Click **OK** and then save your changes.

Related concepts

[Virtual zones and how to restrict VPN access](#) on page 518

[Benefits of using access control rules to direct VPN traffic](#) on page 520

Related tasks

[Configure VPN definitions](#) on page 535

Configure certificate or CA information

Determine if you will use certificates for your VPN.

Steps

- 1) Review the details on certificates and CAs.
- 2) Decide if you will use a public CA server, your private CA server, or self-signed certificates generated by the firewall (which can be used between two firewalls or between a firewall and a VPN client machine).
- 3) Determine if you are using a public or private CA server. You might also want to add remote identities to be used in conjunction with a Certificate Authority policy.
- 4) Review details for using the self-signed certificates if you are using them.
- 5) If you are configuring a VPN between the firewall and VPN client software, and if you are not using a CA, you must create a remote certificate, export it, then import the certificate into the VPN client.

Related concepts

[Managing firewall certificates](#) on page 620

[Managing certificate authorities](#) on page 629

[Managing remote identities](#) on page 633

[Managing remote certificates](#) on page 623

Related tasks

[Export certificates](#) on page 627

Configure VPN definitions

Use the **VPN definitions** window to configure and manage VPN definitions.

Create or modify VPN definitions

Create a new or modify an existing VPN definition.



Note: You cannot create more than 16,383 VPN definitions.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New** or select an existing definition from the list and click **Modify**. The **VPN Properties** window appears.
- 3) Enter the necessary information to create a VPN definition.
- 4) When you are done entering information, save your changes.
- 5) Click **Add** to add the VPN definition to the **VPN Definitions** list.



Note: Use the **Move Up** and **Move Down** arrows to place the new definition in the desired position.

Related tasks

[Configure the General tab on page 539](#)

Related reference

[What you can define on the VPN Properties window on page 520](#)

Delete a VPN definition

Remove a VPN definition that is no longer needed.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the list of VPN definitions, select the VPN definition.
- 3) Click **Delete**.
- 4) Click **Yes** to confirm the deletion of a definition.

Duplicate a VPN definition

Create a copy of an existing VPN definition.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the list of VPN definitions, select the **VPN definition**.

- 3) Click **Duplicate** to create a copy of the VPN definition.



Note: The default name of the new item is Copy_of_x, where x is the original definition's name. To modify the name, select the definition and click **Rename**.

Rename a VPN definition

Change the name of a VPN definition.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the list of VPN definitions, select the VPN definition.

- 3) Click **Rename**. The **VPN Rename** window appears.

- 4) In the **Please enter the new name for this VPN** field, type a name for the definition.

- 5) Click **OK**.

Enable or disable a VPN definition

Multiple VPN definitions can be enabled or disabled at a time.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the list of VPN definitions, select the **VPN definition**.



Tip: To enable or disable multiple consecutive definitions, select the first definition, then press the **Shift** key while selecting the last definition. To select multiple non-consecutive definitions at one time, press the **Ctrl** key while selecting each desired definition.

- 3) Click **Enable** or **Disable**.



Tip: A disabled VPN definition is grayed out in the list.

Move a VPN definition up or down

The firewall processes the list of VPN definitions from the top to the bottom. Make sure your VPN definitions are listed in the appropriate order.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the list of VPN definitions, select the VPN definition.

- 3) Click **Move Up** or **Move Down** to set the matching order of the VPN definitions.



Tip: The first definition that matches a connection request is used to allow or deny that connection.

View VPN status

View the status of all configured VPN definitions.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the list of VPN definitions, select a VPN definition.

- 3) Click **VPN Status**. The **Active VPNs** window appears.

- 4) View the status of all the VPN definitions.



Tip: Click **Refresh Now** to update the information in the **Active VPNs** window.

- 5) Click **Close**.

Configure the General tab

Use the **General** tab to configure basic VPN settings.

Enable a VPN definition

Name and enable the VPN definition.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New** or select an existing definition from the list and click **Modify**. The **VPN Properties** window appears.
- 3) In the **Name** field, type the name of this VPN.
- 4) In the **Enabled** options, select **Yes** to enable this VPN definition.

Select the mode and client address pool

Choose the VPN mode and determine if you are using a client address pool.

Steps

- 1) From the **Mode** drop-down list, select the mode.



Tip: For option descriptions, click **Help**.

- 2) [Conditional] If you want remote peers to make connections using only the IP addresses contained within one of the available client address pools, select a client address pool from the **Client Address Pool** drop-down list.

Choose the IKE version, encapsulation method and zone

Configure the IKE version, the encapsulation method, and the zone to terminate on.

Steps

- 1) [Conditional] If you are using automatic key exchange, select which **IKE** version to use.



Tip: For option descriptions, click **Help**.

- 2) In the **Encapsulation** field, select **Tunnel** or **Transport** in the **General** tab.

- 3) From the **Zone** drop-down list, select the zone you want to assign this VPN to.



Note: The firewall terminates each VPN in a zone so that access control rules can be applied to the VPN.

Choose the IP version and addresses

Configure the IP version and network addresses.

Steps

- 1) [Conditional] If IPv6 is enabled, use the IP version options to select which type of IP address your VPN definition will use.



Tip: For option descriptions, click **Help**.

- 2) In the **Local IP** field, indicate which IP address to use as the local gateway. Select one of the following:
 - **Use Localhost IP** — Select this option to have the firewall assign the IP address. The firewall uses its routing table to automatically determine which interface or alias address is associated with a route to reach the remote gateway
 - **Specify IP** — Select this option to configure a specific IP address. This IP address should be one of the firewall's interface or alias addresses, and that interface must have a route to reach the remote gateway.



Note: If configuring a VPN for an HA cluster, be sure to use the localhost option or specify an alias shared by the cluster.

- 3) To add or modify a local network address to the Local Network/IP list, click **New** or select an address from the list and click **Modify**. The **Local Network List** window appears.
 - a) In the **IP Address** field, type the IP address used in this VPN definition.
 - b) In the **Number of bits in Netmask** field, use the up/down arrows to select the number of bits that are significant in the network mask. The value specified is used to identify the network portion of the IP address.



Note: The **Local Network/IP** list shows the network names or IP addresses the firewall can use in a VPN definition. The addresses in this list and the addresses in the **Remote Network/IP** list together identify allowed and reachable addresses for this VPN tunnel.

- 4) [Conditional] In the **Remote IP** field, type the IP address of the remote peer.



Note: This field is available for **Fixed IP** and **Manually Keyed VPN** mode.

- 5) [Conditional] Add or modify an entry in the **Remote Network / IP** list.



Note: This option is available only for **Fixed IP**, **Manually Keyed VPN**, and **Bypass** modes.

- a) Click **New** or select an address in the list and click **Modify**. The **Remote Network List** window appears:
- b) In the **IP Address** field, type the IP address used in the VPN definition.

- c) In the **Number of bits in Netmask** field, use the up/down arrows to select the number of bits that are significant in the network mask. The value specified is used to identify the network portion of the IP address.



Note: The networks configured here represent real networks located behind the remote VPN peer. The addresses in this list and the addresses in the **Local Network/IP** list together identify allowed and reachable addresses for this VPN tunnel.

- 6) [Conditional] If the Mode is **Dynamic IP Restricted Client**, you can add or modify an entry in the **Dynamic Virtual Address Range** list.
 - a) Click **New** or select an address range and click **Modify**. The **Dynamic Virtual Address Range List** window appears.
 - b) In the **IP Address** field, type the IP address range a client can use when initiating a VPN connection.
 - c) In the **Number of bits in Netmask** field, use the up/down arrows to select the number of bits that are significant in the network mask. The value specified is used to identify the network portion of the IP address.
- 7) [Optional] In the **Comments** field, type a short description for the VPN definition.
- 8) Click **Add**.

Related concepts

[Virtual zones and how to implement them](#) on page 518

Related tasks

[Choose the IKE version, encapsulation method and zone](#) on page 539

Related reference

[Example VPN Scenarios](#) on page 522

Configure the Remote Authentication tab

Use the Remote Authentication tab to configure remote authentication settings.

Define the remote peer's identity and password

Configure identity settings for the remote peer.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New** or select an existing definition from the list and click **Modify**. The **VPN Properties** window appears.
- 3) Click the **Remote Authentication** tab.
- 4) From the **Remote Authentication Method** drop-down list, select **Password**.
- 5) Use either of these methods to create the password:
 - In the **Enter Remote Password** field, type the password, and then retype the password in the **Verify Remote Password** field to confirm it.
 - Click **Generate** to create a strong password that will populate the **Enter Remote Password** and **Verify Remote Password** fields.
- 6) In the **Remote Identity** area, select an identity the remote peer will be required to use to authenticate to the firewall. The firewall uses this information to determine the password the remote peer should use.
 - Select **Gateway IP Address (not specified)** to require the remote peer to use its gateway address as its identity to authenticate to the firewall.
 - Select **Remote One or More Remote IDs From List** to require the remote peer to use the configured remote identity.



Note: The remote identity is optional for Fixed IP VPN definitions because the firewall can use the IP address to determine who the remote peer is and thus what password the remote peer should be using.

- 7) [Optional] Click **Remote Identities** to create a new remote identity. The **Remote Identities** window appears. Create the new identity, then click **OK** to return to the **Remote Authentication: Password** view.

Define the Certificate and Certificate Authority

Configure remote certificate settings using a Certificate Authority.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New** or select an existing definition from the list and click **Modify**. The **VPN Properties** window appears.
- 3) Click the **Remote Authentication** tab.
- 4) From the **Remote Authentication Method** drop-down list, select **Certificate+Certificate Authority**.
- 5) From the **Certificate authorities** drop-down list, select a Certificate Authority or CA group to use for this VPN definition.



Note: The remote VPN peer is required to use a certificate that was signed by one of the configured CAs or CA groups for this VPN definition.

- 6) Click **Certificate Authorities** to add a CA or CA group to this list. The **Certificate Authorities** window appears.



Note: You can add several Certificate Authorities to this list.

- 7) In the **Remote Identities** area, select a remote identity.
- 8) [Optional] Click **Remote Identities** to create a new remote identity. The **Remote Identities** window appears. Create the new identity, then click **OK** to return to the **Remote Authentication: Certificate + Certificate Authority** view.



Note: You can add several remote identities to this list.

Related concepts

[Managing certificate authorities](#) on page 629

[Managing remote identities](#) on page 633

Define the single certificate

Configure remote certificate settings using a single certificate.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New** or select an existing definition from the list and click **Modify**. The **VPN Properties** window appears.
- 3) Click the **Remote Authentication** tab.
- 4) From the **Remote Authentication Method** drop-down list, select **Single Certificate**.
- 5) From the **Remote Certificate** drop-down list, select the certificate used.
- 6) [Optional] Click **Remote Identities** to create a new remote identity. The **Remote Identities** window appears. Create the new identity, then click **Close** to return to the **Remote Authentication: Single Certificate** view.



Note: You can add several remote certificates to this list.

Related concepts

[Managing remote certificates](#) on page 623

Related tasks

[Import firewall certificates](#) on page 622

Implement extended authentication for VPN

Extended authentication requires VPN users to provide a set of credentials before they can access the VPN. The credentials can be for local firewall users or for users on an external authentication server such as Active Directory.



Note: Extended authentication must also be enabled on the remote client. See your client software documentation for information on configuring and enabling extended authentication.

Steps

- 1) Specify the authentication method(s) that are available on your firewall:
 - a) Select **Network > VPN Configuration > ISAKMP Server**. The **ISAKMP Server** window appears.

Tip: For option descriptions, click **Help**.
 - b) In the **Allowed XAUTH Methods** field, select the **Password** checkbox to enable one or more methods.
 - c) Save the changes.
- 2) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.
- 3) Click **New** or select an existing definition from the list and click **Modify**. The **VPN Properties** window appears.
- 4) Click the **Remote Authentication** tab. From the **Remote Authentication Method** drop-down list select **XAUTH**.
- 5) From the **Remote identities** list, select the identities that will use extended authentication to authenticate to the firewall.



Note: A check mark appears next to selected remote identities.

- 6) [Optional] Click **Remote Identities** to create a new remote identity. The **Remote Identities** window appears. Create the new identity, then click **OK** to return to the **Remote Authentication: Certificate + Certificate Authority** view.



Note: You can add several remote certificates to this list.

Related concepts

[Managing remote identities](#) on page 633

Related tasks

[Configure the ISAKMP server](#) on page 557

Related information

[Validating users and user groups](#) on page 93

Configure the Local Authentication tab

Use the **Local Authentication** tab to configure local authentication settings.

Define the password

Set the password for the VPN.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New** or select an existing definition from the list and click **Modify**. The **VPN Properties** window appears.
- 3) Click the **Local Authentication** tab.
- 4) [IKEv2 definition only] From the **Local Authentication Method** drop-down list, select **Password**.
- 5) Create the password the firewall uses to authenticate to the remote peer.
Use either of these methods to create the password:
 - In the **Enter Remote Password** field, type the password, and then retype the password in the **Verify Remote Password** field to confirm it.
 - Click **Generate** to create a strong password that will populate the **Enter Remote Password** and **Verify Remote Password** fields.



Note: If Password is the remote authentication method, these fields are automatically populated with the remote password and cannot be modified here.

- 6) From the **Local Identity Type** drop-down list, select the type of identity to use when identifying the firewall to the remote peer.
- 7) In the **Value** field, type the actual value used as the firewall identity.
The value must be of the type selected as the **Local Identity Type**. For example, if you selected **IP Address** in the **Local Identity Type** drop-down list, you must type an IP address in the **Value**
- 8) Click **OK**.

Define a certificate

Define the certificate and local identity for the VPN.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New** or select an existing definition from the list and click **Modify**. The **VPN Properties** window appears.
- 3) Click the **Local Authentication** tab.
- 4) [IKEv2 definition only] From the **Local Authentication Method** drop-down list, select **Certificate**.
- 5) From the **Local certificate** drop-down list, select the certificate used firewall.
- 6) Create or import a certificate for this definition.
 - a) Click **Local Certs**. The **Firewall Certificates** window appears.
 - b) Create or import the new certificate, then click **Close** to return to the **Local Authentication: Certificate** view.



Note: You can add several remote certificates to this list.

- 7) From the **Local Identity type** drop-down list, select the type of identity to use when identifying the firewall to the remote peer.



Note: Only those identities defined within the selected certificate will be available in this field.

The **Local Identity value** field contains the available identity values associated with the selected identity type and with the local certificate.

- 8) Click **OK**.

Related concepts

[Managing remote certificates](#) on page 623

Related tasks

[Import firewall certificates](#) on page 622

Configure the Crypto tab

Use the **Crypto** to configure encryption settings for the VPN.

Configure manual authentication for VPN definition

Configure manual key exchange options.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) From the **IPSEC transformations** drop-down list, select the appropriate form of IPsec transformation.

- From the **Encryption** drop-down list, select the type of encryption you and the remote peer have chosen to use. The choices are:

Table 93: Encryption options Encryption options

Encryption type	Key length
aes256	256-bit
3des	168-bit
aes128	128-bit
cast128	128-bit
des	56-bit
null	0

- In the **Authentication hash** drop-down list, select the type of authentication you and the remote peer have chosen to use.
- Click **Generate Keys** to create keys and SPI index values. Randomly generated keys appear in the key and SPI fields.
 - The key and SPI fields available are dependent on the IPSEC Transformations selection.
 - You can type your own unique key and SPI index. Since manually generating random keys is difficult, the firewall provides randomly generated authentication and encryption keys and Security Parameters Index (SPI) value for you and the remote peer to use. We recommend that you use the default keys.



Note: Once you have chosen the keys, they must be kept secure. You must only exchange the keys by a secure method, such as diskette, encrypted e-mail (such as PGP), or via the telephone. If attackers learn the key, they can decrypt all of your VPN traffic.

- Click **OK**.
- Send the generated keys and SPI values to the remote peer via a secure method (diskette, encrypted e-mail, or telephone).

The remote peer must enter the inbound and outbound keys and SPIs in the opposite fields:

Table 94: Key relationship between the firewall and the remote peer

If the key on the Sidewinder is in this field:	That key is entered on the remote peer in this field:
AH inbound key and SPI	AH outbound key and SPI
AH outbound key and SPI	AH inbound key and SPI
ESP inbound key and SPI	ESP outbound key and SPI
ESP outbound key and SPI	ESP inbound key and SPI

Define cryptographic and hashing algorithms

Define the algorithms used in an automatic key exchange.

Steps

- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New** or select an existing definition from the list and click **Modify**. The **VPN Properties** window appears.
- 3) Click the **Crypto** tab.
- 4) From the **IPSEC encryption algorithms** list, select an algorithm.



Note: You can select multiple algorithms.

- The null option contains an encryption header, but does not specify an encryption algorithm. It is generally used during testing.
- To authenticate only, without performing encryption, deselect all encryption algorithms.

- 5) From the **IPSEC authentication algorithms** list, select an algorithm.



Note: You can select multiple algorithms.

- 6) Click **OK**.

Configure the Advanced tab

Define the advanced options for a VPN definition under the **Advanced** tab.



CAUTION: Only administrators who know the complexities of VPN must modify the information on this tab.

Steps


- 1) Select **Network > VPN Configuration > VPN Definitions**. The **VPN Definitions** window appears.





Tip: For option descriptions, click **Help**.


- 2) Click **New** or select an existing definition from the list and click **Modify**. The **VPN Properties** window appears.
- 3) Click the **Advanced** tab.
- 4) In the **Internet Key Exchange (IKE)** area select the **IKE v1 exchange type**.

- 5) Define the **Hard limits** and **Soft percentage**.
- 6) Select the algorithms and key exchange groups.
 - From the **Encryption Algorithms** list, select the encryption algorithm(s) to use during Phase 1.
 - From the **Hash Algorithms** list, select the hash algorithm(s) to use during Phase 1.
 - From the **PRF Algorithms** list, select the PRF algorithm(s) to use during Phase 1 (IKEv2 only).
 - From the **Key Exchange Groups** list, select the Diffie-Hellman group to use for the derivation of ISAKMP keys.
- 7) Select these options based on the need.
 - **Force XAuth on rekey** — Select this option to force XAuth to be performed each time the phase 1 session is started or renegotiated.
 - **Relax strict identity matching** — Select this option to relax the identity matching restrictions. If you are experiencing issues associated with identity processing with the remote VPN peer, selecting this option can improve interoperability, but decreases security.
 - **Enable NAT traversal (NAT-T)** — Select this option to allow multiple VPN users behind a NAT device to access a VPN tunnel.
 - **Enable initial contact** — Select this option to send and receive initial contact notify messages when first connecting with a VPN peer. This causes the peer to reload any previous state and is useful for re-synchronizing state after a device restart.
 - **Encrypt final aggressive mode packet** — For aggressive mode IKEv1 exchanges, this option will cause the firewall to encrypt the final aggressive mode packet in the exchange.

 **Tip:** You might need to enable this option if you are experiencing interoperability issues with your VPN peer using aggressive mode.
 - **Enable dead peer detection** — [If IKEv2 is the selected mode] Select this option to send and receive messages to a VPN peer at regular intervals to confirm that the peer is available.

 **Note:** If a reply is not received for a period of time, the connection with the peer is ended and no traffic is sent to the peer. The VPN connection must be re-established to send traffic to the peer.
- 8) In the **Rekey** area, define the **Hard lifetimes** and **Soft percentage**.
- 9) Select these options based on the need.
 - **Forced rekey** — Select this option to force the connection to rekey when the limits are reached, even if no traffic has passed through the VPN since the last rekey.

 **CAUTION:** Do not enable the **Forced rekey** option if you have HA/LS configured and are using static IP addresses for your VPNs. Doing so will cause all firewalls in the cluster to attempt to instantiate the VPN at the same time, resulting in failure.
 - **Enable extended sequence numbers** — Select this option to double the IPsec sequence number to a 64-bit number.

 **Tip:** This option is useful if you expect extremely heavy traffic, ensuring that you can pass traffic over a VPN without running out of sequence numbers.
 - **(Perfect forward secrecy (PFS))** — Select this option to ensure that the key material associated with each IPsec security association cannot be derived from the key material used to authenticate the remote peer during the ISAKMP negotiation.
 - **Oakley group** — Select the Diffie-Hellman group to use for the PFS derivation of IPsec keys.



Note: This option is available only if the PFS option is enabled.

- 10) Click **OK**.

Configure a client address pool

Create a client address pool for use in a VPN definition.



Note: Client address pools are not allowed in definitions that use IPv6 addresses.

Create a client address pool

Use the **Client Address Pools** window to create a new client address pool.

Steps

- 1) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New**. The **New Pool** window appears.
- 3) In the **Pool Name** field, type the name of the new address pool.
- 4) In the **Virtual Subnet** field:
 - a) Type the IP address that defines the network portion of the IP addresses used in the client address pool.
 - b) In the netmask field, specify the number of bits to use in the network mask. The network mask specifies the significant portion of the IP address.



Note: Configure routing on the protected networks so that traffic destined for the virtual subnet is routed to the Sidewinder.

- 5) Click **Add** to add the new client address pool.

Delete a client address pool

Remove a client address pool that is no longer needed.

Steps

- 1) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Pools** list, select the address pool.
- 3) Click **Delete**.
- 4) Click **Yes** to confirm the deletion.

Configure the Subnets tab

Configure the networks for the client address pool.

Configure the Virtual Subnet List

Sidewinder uses the **Virtual Subnet List** to reassign IP addresses on connections from remote peers.



Note: The virtual subnets should *not* match the internal network's subnet, as this configuration could cause internal routing and connectivity issues. Virtual addressing works only if the client address pool uses unassigned address space.

Steps

- 1) Create a virtual subnet.
 - a) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.



Tip: For option descriptions, click **Help**.

- b) From the **Pools** list, select an address pool or click **New** to create an address pool.
- c) In the **Subnets** tab, click **New**. The **New Virtual Subnet** window appears.
- d) In the **Virtual Subnet** field, enter the IP address that defines the network portion of the IP addresses used in the client address pool.



Note: The virtual subnet cannot exist in the firewall's routing table.

- e) In the netmask field, specify the number of bits to use in the network mask. The network mask specifies the significant portion of the IP address.

- f) Click **Add**.
- 2) Modify a virtual subnet.
 - a) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.
 - b) From the **Pools** list, select an address pool.
 - c) Click **Subnets** tab. From the **Virtual Subnet** list, select an entry.
 - d) Click **Modify**. The **Modify Virtual Subnet** window appears.
 - e) In the **Virtual Subnet** field, modify the IP address.
 - f) In the netmask field, specify the number of bits to use in the network mask.
 - g) Click **OK**.
 - 3) Delete a virtual subnet.
 - a) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.
 - b) From the **Pools** list, select an address pool.
 - c) Click **Subnets** tab. From the **Virtual Subnet** list, select an entry.
 - d) Click **Delete**.

Configure the Local Subnet List

Configure the local networks for the VPN.

Steps

- 1) Create a local subnet.
 - a) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.



Tip: For option descriptions, click **Help**.

- b) From the **Pools** list, select an address pool or click **New** to create an address pool.
- c) In the **Subnets** tab, click **New**. The **New Local Subnet** window appears.
- d) In the **Local Subnet** field, enter the IP address that defines the network portion of the IP addresses used in the client address pool.



Note: The virtual subnet cannot exist in the firewall's routing table.

- e) In the netmask field, specify the number of bits to use in the network mask. The network mask specifies the significant portion of the IP address.
 - f) Click **Add**.
- 2) Modify a local subnet.
- a) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.
 - b) From the **Pools** list, select an address pool.
 - c) Click **Subnets** tab. From the **Local Subnet** list, select an entry.
 - d) Click **Modify**. The **Modify Local Subnet** window appears.
 - e) In the **Modify Subnet** field, modify the IP address.
 - f) In the netmask field, specify the number of bits to use in the network mask.
 - g) Click **OK**.
- 3) Delete a local subnet.
- a) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.
 - b) From the **Pools** list, select an address pool.
 - c) Click **Subnets** tab. From the **Local Subnet** list, select an entry.
 - d) Click **Delete**.

Related tasks

[Configure the Servers tab](#) on page 553

[Manage the fixed IP map](#) on page 556

Configure the Servers tab

Use the **Servers** tab to configure DNS and NBNS/WINS servers.

Manage the DNS servers

Create, modify or delete the DNS servers for the client address pool.

- Create a DNS server
 - 1) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Pools** list, select an address pool or click **New** to create an address pool.
- 3) In the **Servers** tab, click **New**. The **New DNS server** window appears.
- 4) In the **DNS Server** field, enter the IP address that specifies the location of the DNS server.



Tip: Click **DNS Lookup** to search for a hostname.

- 5) Click **Add**.
- Modify a DNS server
 - 1) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.
 - 2) From the **Pools** list, select an address pool.
 - 3) Click **Servers** tab. From the **DNS servers** list, select a **DNS** server.
 - 4) Click **Modify**. The **Modify DNS Server** window appears.
 - 5) In the **DNS server** field, modify the IP address or click **DNS Lookup** for a different address.
 - 6) Click **OK**.
 - Delete a DNS server
 - 1) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.
 - 2) From the **Pools** list, select an address pool.
 - 3) Click the **Servers** tab. From the **DNS servers** list, select a DNS server.
 - 4) Click **Delete**.

Manage the NBNS/WINS servers

Create, modify, or delete the NBNS/WINS servers for the client address pool.

Steps

- 1) Create an NBNS/WINS server.
 - a) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.



Tip: For option descriptions, click **Help**.

- b) From the **Pools** list, select an address pool or click **New** to create an address pool.

- c) In the **Servers** tab, click **New**. The **NBNS/WINS server** window appears.
- d) In the **NBNS/WINS Server** field, enter the IP address that specifies the location of the NBNS/WINS server.



Tip: Click **NBNS/WINS Lookup** to search for a hostname.

- e) Click **Add**.

2) Modify an NBNS/WINS server.

- a) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.
- b) From the **Pools** list, select an address pool.
- c) Click **Servers** tab. From the **NBNS/WINS servers** list, select an NBNS/WINS server.
- d) Click **Modify**. The **Modify NBNS/WINS Server** window appears.
- e) In the **NBNS/WINS Server** field, modify the IP address or click **NBNS/WINS Lookup** for a different address.
- f) Click **OK**.

3) Delete an NBNS/WINS server.

- a) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.
- b) From the **Pools** list, select an address pool.
- c) Click the **Servers** tab. From the **NBNS/WINS servers** list, select an NBNS/WINS server.
- d) Click **Delete**.

Related tasks

[Configure the Subnets tab](#) on page 551

[Manage the fixed IP map](#) on page 556

Manage the fixed IP map

Fixed IP mappings allow you to associate an identification string to a particular client IP address.

Create a fixed IP map

Define a new fixed IP client mapping address.

Steps

- 1) Select **Network > VPN Configuration > Client Address Pools** . The **Client Address Pools** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Pools** list, select an address pool or click **New** to create an address pool.
- 3) In the **Fixed IP Map** tab, click **New**. The **Pool Entry** window appears.
- 4) In the **IP Address** field, enter the fixed IP address that will be associated with this mapping.



Note: Click **DNS Lookup** to search for a hostname.

- 5) Click **New** to add a new client identifier. The **New Client ID** window appears.
- 6) In the **Client ID** field, enter a client ID and click **OK**.
- 7) Click **Add** to add the new pool entry to the list.

Modify a fixed IP map

Modify a fixed IP client mapping address.

Steps

- 1) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Pools** list, select an address pool.
- 3) Click **Fixed IP Map** tab. From the **Fixed IP Client Address Mappings** list, select an IP address.
- 4) Click **Modify**. The **Modify Pool Entry** window appears.
- 5) In the **IP Address** field, modify the IP address or click **DNS Lookup** for a different address.
- 6) From the **Client Identification Strings** list, select a client identifier.

- 7) Click **Modify**. The **Modify Client ID** window appears.
- 8) In the **Client ID** field, enter a client ID and click **OK**.
- 9) Click **Add**.

Delete a fixed IP map

Delete a fixed IP client mapping address.

Steps

- 1) Select **Network > VPN Configuration > Client Address Pools**. The **Client Address Pools** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Pools** list, select an address pool.
- 3) Click **Fixed IP Map** tab. From the **Fixed IP Client Address Mappings** list, select an IP address.
- 4) Click **Delete**.
- 5) Click **Yes** to confirm deletion.

Configure the ISAKMP server

Configure ISAKMP server properties such as XAUTH, connection settings, and the audit level.

Select the audit level

Increase or decrease the audit level of the ISAKMP server. Higher audit levels can be useful for troubleshooting VPN issues.

Steps

- 1) Select **Network > VPN Configuration > ISAKMP Server**. The **ISAKMP Server** window appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Audit Level** drop-down list, select the type of audit output for the ISAKMP server.

Configure the Advanced ISAKMP Options window

Configure advanced certificate and connection settings for the ISAKMP server.

Steps

- 1) In the **Advanced ISAKMP Server Options** area, click **Properties**. The **Advanced ISAKMP Options** window appears.



Tip: For option descriptions, click **Help**.

- 2) Configure the following options.

- **Allow certificate negotiation** — The default is to allow certificate negotiation. If you deselect the checkbox, all certificates used to authenticate remote peers must either be in the local certificate database or be accessible via LDAP.
- **Retry negotiation after <value> seconds and Maximum negotiation attempts** — Set how long (in seconds) the ISAKMP server will wait for a response from its request to a remote peer before resending the packet and how many times it will attempt to resend a packet if no response is received.
- **Allow <value> new connections to the ISAKMP Server at one time** — Select how many remote peers can establish a connection to the ISAKMP server at one time. The default is unlimited.



Note: If you have a large number of remote users whose sessions will immediately reconnect after restart, you might experience issues with re-establishing the connection and should adjust this limit.

- **Allow expired certificates** — Select whether you will allow expired certificates.
 - **Perform certificate revocation checking** — If certificate revocation lists (CRLs) are configured for your Certificate Authorities, select this checkbox to check for revoked certificates.
 - **Allow certificates with unknown status** — If you are checking for revoked certificates, select whether to allow certificates with unknown status. If you select **No**, up-to-date CRLs must be available on the firewall for all certificates and associated certificate authorities during certificate validation. If a needed CRL is not present, certificate validation will fail and the associated VPN session will not be established.
- 3) Click **OK** to close the **Advanced ISAKMP Options** window.

Configure the XAUTH Configuration area

Configure extended authentication settings.

Steps

- 1) In the **XAUTH (Extended Authentication) Configuration** area, configure how the ISAKMP server interacts with extended authentication.



Tip: For option descriptions, click **Help**.

- a) In the **Allowed XAUTH Methods** area, select the authentication methods you want available for VPN definitions that use extended authentication. A check-mark indicates an allowed authentication method. To add an authentication method to the list, click **New** and select a method from the pop-up menu. Configure the authenticator in the **New Authenticator** pop-up window.

- b) If two or more authentication methods are selected, specify a default method from the **Default XAUTH Method** drop-down list.



Note: If you do not specify a default method, the first method selected in the list is used.

- c) Click **Properties** to open the **Advanced XAUTH Options** window and configure the following:
 - **Allow only one VPN per XAUTH authenticated user** — Select this checkbox to limit the number of active VPNs to one per user. The default is one active VPN per authenticated user. This limit should work for most security policies.



CAUTION: If your policy allows multiple users to use the same user name, generally from different VPN clients, you might need to remove this limit. We recommend that you do not allow more than one user per user name.

- c) In the **Negotiation Properties** area, configure these options.
 - **Retry negotiation after x seconds** — Set how long (in seconds) the ISAKMP server will wait for a response to its request to an authenticator before resending the packet.
 - **Maximum negotiation attempts** — Set how many times the server will attempt to resend a packet if no response is received.
- d) Click **OK** to close the **Advanced XAUTH Options** window.

- 2) Save the changes.

Related concepts

[Authenticator configuration](#) on page 100

Related tasks

[Configure certificate or CA information](#) on page 535

PART V

Maintenance

Contents

- [Administration management](#) on page 563
- [General maintenance](#) on page 575
- [Certificate/key management](#) on page 617
- [High Availability](#) on page 639

Administration management

Contents

- [Management options](#) on page 563
- [Admin Console access management](#) on page 565
- [Command line interface access management](#) on page 567


Manage Sidewinder using the Admin Console, command line interface, or Forcepoint Sidewinder Control Center.

Management options

You can manage Sidewinder in several ways.

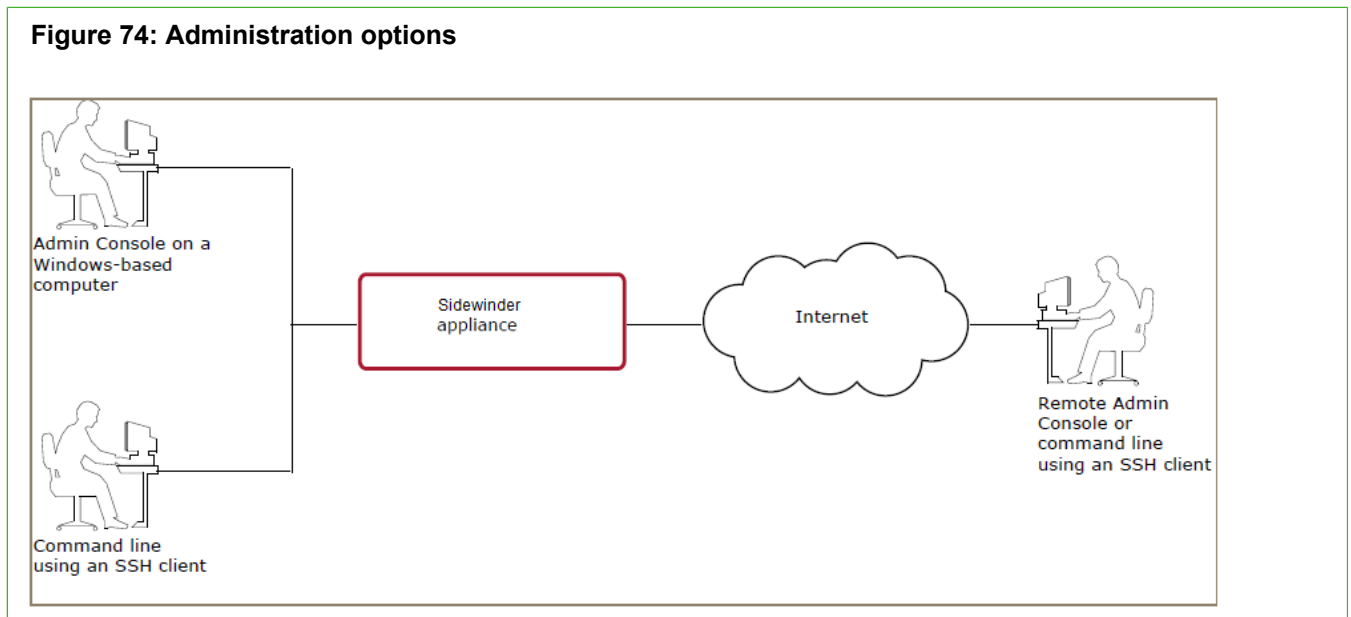
- Admin Console
- Command line interface
- Forcepoint Sidewinder Control Center

Table 95: Methods for managing Sidewinder

Method	Description
Admin Console	<p>The Sidewinder Admin Console is graphical software that runs on a Windows-based computer within your network.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> Note: The Admin Console is occasionally referred to as cobra in some command line tools.</p> </div>

Method	Description
Command line interface	<p>If you are experienced with UNIX, you can use the command line interface to perform most configuration and management tasks. Command line interface refers to any UNIX prompt. The command line interface supports many firewall-specific commands as well as standard UNIX commands. For example, the <code>cf</code> command can perform a wide range of configuration tasks. For help using the command line interface, refer to the Manual (<code>man</code>) pages included on the firewall:</p> <ol style="list-style-type: none"> 1) Log on to the firewall at a command prompt. 2) Type <code>man</code> followed by the name of a command. For example: <code>man cf</code>. 3) Press Enter.
Sidewinder Control Center	<p>Sidewinder Control Center, an enterprise-class management appliance, allows you to centrally manage multiple Sidewinder appliances. See the <i>Forcepoint Sidewinder Control Center Product Guide</i> available at https://support.forcepoint.com</p>

Regardless of the method, you can manage the firewall from a number of locations. The figure highlights the administration options available to you.



Consider the following:

- A rule is required to allow access for the zone the management computer resides in.
- The remote administration methods do not support IPv6.
- If the firewall enters emergency maintenance mode, all remote administration methods are disabled. In this situation, use the local console to access the command line interface.

Related concepts

[Admin Console access management](#) on page 565

[Command line interface access management](#) on page 567

[What the Admin Console does](#) on page 53

Related tasks

[Install the Management Tools](#) on page 42

Admin Console access management

Use the Admin Console to manage your firewall. The Admin Console is version-specific and must be installed on a Windows-based computer.

Refer to the table to determine which Admin Console version is appropriate for your firewall.

Table 96: Admin Console and firewall versions

Use this Admin Console	To manage this firewall version
5.x	8.x
4.x	7.x

The Admin Console connects to the firewall using an SSL connection. A default SSL certificate containing the firewall host name is initially assigned to the firewall Admin Console server.

Related tasks

[Configure Admin Console properties](#) on page 565

[Manage Admin Console access](#) on page 566

Configure Admin Console properties

Configure Admin Console properties such as the logon greeting and SSL certificate used.

Select **Maintenance > Remote Access Management**. The **Admin Console Properties** tab appears.



Tip: For option descriptions, click **Help**.

You can perform the following tasks:

Table 97: Admin Console properties tasks

Task	Steps
Select a different SSL certificate	<ol style="list-style-type: none"> 1) From the SSL certificate drop-down list, select the appropriate firewall certificate. 2) Save your changes.
Create a logon greeting	<ol style="list-style-type: none"> 1) In the Login greeting text field, type the text you want to appear when a user logs on using the Admin Console. 2) [Optional] To always display the logon greeting for each logon, select Display the login greeting regardless of user preferences. 3) Save your changes.
Remove a logon greeting	<ol style="list-style-type: none"> 1) Clear the Login greeting text field. 2) Save your changes.

Manage Admin Console access

Admin Console access is controlled using access control rules. By default, Admin Console access is enabled for the internal zone.

You can modify the default **Admin Console** rule or create new rules as necessary.

Table 98: Admin Console access tasks

Task	Steps
Modify the default Admin Console rule	<ol style="list-style-type: none"> 1) Select Policy > Access Control Rules. 2) Expand the Administration rule group. 3) Select the Admin Console rule, then click Modify. 4) Modify the rule as necessary, then click OK. 5) Save your changes.

Task	Steps
Create a new Admin Console rule	<ol style="list-style-type: none"> 1) Select Policy > Access Control Rules. 2) Click New > New Rule. 3) Make the following selections: <ul style="list-style-type: none"> • Applications — Select Admin Console. • Source Zone — Select the zone that contains the Admin Console computer. • Destination Zone — Select the zone that contains the Admin Console computer. • Users and Groups — Select <Authenticated>. • NAT — Select <localhost>. • Redirect — Select <Firewall> (IP). • Redirect port — Type 9002. • Authenticator — Select an authentication method. 4) Configure the other rule settings as necessary, then click OK. 5) Save your changes.

Command line interface access management

The command line interface can be reached using Secure Shell management or local management.



Note: Telnet management can also be enabled by creating a Telnet Server rule. However, we do not recommend using Telnet because it poses a security risk.

Related concepts

[Secure Shell management](#) on page 567

[Local management](#) on page 573

Secure Shell management

Secure Shell (SSH) provides secure encrypted communication between two hosts over a network that is not secure, allowing you to securely manage your firewall from a remote location.

The firewall can act as an SSH server, an SSH client, or both.

Consider the following information about SSH on the firewall.

- The firewall SSH server and client are based on the OpenSSH implementation.
- SSH version 1.5 and 2.0 sessions are supported.
- sftp and sftp-server are included in OpenSSH and installed on the firewall.
- There are two SSH configuration files:
 - SSH server: `/etc/ssh/sshd_config`
 - SSH client: `/etc/ssh/ssh_config`

See the `ssh`, `sshd`, `ssh_config`, `sshd_config`, and `ssh-keygen` man pages for additional details.

Manage SSH access

Access to the firewall SSH server is controlled using access control rules. You can modify the default Secure Shell Server rule or create new rules as necessary.



Tip: For option descriptions, click **Help**.

Table 99: Admin Console access tasks

Task	Steps
Modify the default Secure Shell Server rule	<ol style="list-style-type: none"> 1) Select Policy > Access Control Rules. 2) Expand the Administration rule group. 3) Select the Secure Shell Server rule, then click Modify. 4) Modify the rule as necessary, then click OK. 5) Save your changes.

Task	Steps
Create a new Secure Shell Server rule	<ol style="list-style-type: none"> 1) Select Policy > Access Control Rules. 2) Click New > New Rule. 3) Make the following selections: <ul style="list-style-type: none"> • Applications — Select SSH Server. • Source Zone — Select the zone that contains the SSH client. • Destination Zone — Select the zone that contains the SSH client. • Users and Groups — Select <Authenticated>. • NAT — Select <None>. • Redirect — Select <None>. • Authenticator — Select an authentication method. 4) Configure the other rule settings as necessary, then click OK. 5) Save your changes.

Connect to an SSH server from the firewall command line interface

The firewall can act as an SSH client, allowing you to connect to an SSH server from the command line interface. For example, you might want to establish an SSH connection between two firewalls. In this case one firewall operates as the server (using the SSH server), and the other operates as an SSH client.

To connect to an SSH server from the firewall:

Steps

- 1) At a Sidewinder command prompt, enter the following command to switch to the Admn role:

```
role
```
- 2) Establish the connection with the SSH server by typing one of the following commands:
 - `ssh -l login_name address`
 - `ssh login_name@address`

Where `login_name` is a valid user name on the SSH server and `address` is the host name or IP address of the SSH server.

Result



Tip: When connecting to another Sidewinder, you have the option to specify an authentication method other than the default method. Type a colon and the name of the authentication method after the `login_name` field. For example, to use an authenticator on the firewall called ActiveDirectory, you would type `ssh -l login_name:ActiveDirectory address`. See the `ssh` man page for details.

Configuring SSH-2 public key authentication for SSH

The Sidewinder SSH server and SSH client support RSA, DSA, and ECDSA (elliptic curve DSA) authentication, which use an exchange of public and private keys between the server and the client.

SSH public/private key pairs identify hosts or individuals:

- SSH server key pairs represent the firewall.
- SSH client key pairs represent the administrator who is connecting from the firewall to another SSH server.

Table 100: SSH key files

Type	Keys directory	Version 1.5 key files	Version 2.0 key files
server	/etc/ssh	<ul style="list-style-type: none"> • RSA public key: <code>ssh_host_key.pub</code> • RSA private key: <code>ssh_host_key</code> 	<ul style="list-style-type: none"> • RSA keys: <ul style="list-style-type: none"> • Public: <code>ssh_host_rsa_key.pub</code> • Private: <code>ssh_host_rsa_key</code> • DSA keys: <ul style="list-style-type: none"> • Public: <code>ssh_host_dsa_key.pub</code> • Private: <code>ssh_host_dsa_key</code> • ECDSA: <ul style="list-style-type: none"> • Public: <code>ssh_host_ecdsa_key.pub</code> • Private: <code>ssh_host_ecdsa_key</code>
client	/home/ username/.ssh where username is the administrator's user name	<ul style="list-style-type: none"> • RSA public key: <code>identity.pub</code> • RSA private key: <code>identity</code> 	<ul style="list-style-type: none"> • RSA keys: <ul style="list-style-type: none"> • Public: <code>id_rsa.pub</code> • Private: <code>id_rsa</code> • DSA keys: <ul style="list-style-type: none"> • Public: <code>id_dsa.pub</code> • Private: <code>id_dsa</code> • ECDSA: <ul style="list-style-type: none"> • Public: <code>id_ecdsa.pub</code> • Private: <code>id_ecdsa</code>

Configure SSH-2 public key authentication for the firewall SSH server

Enable RSA, DSA, or ECDSA authentication for the firewall SSH server.

Steps

- 1) Configure the SSH server.
 - a) Select **Maintenance > Remote Access Management**, then click the **SSH Server Properties** tab.



Tip: For option descriptions, click **Help**.

- b) Verify that **Allow SSH-2 public key authentication** is selected.
- c) [Optional] Generate a new SSH host key pair.
 - Click **Generate new host keys**.
 - Click **Yes** to confirm.
 - Click **OK** to acknowledge that the new key pair has been created.



Note: The default host keys are generated during initial firewall configuration.

- d) Save your changes.
- 2) On the SSH server firewall, create an `authorized_keys` file for each administrator.
 - a) At the firewall command line interface, log on.
 - b) Type `srole`, then press **Enter**.
 - c) Run the following commands for each administrator. Press **Enter** after each command.

```
mkdir -p /home/username/.ssh
touch /home/username/.ssh/authorized_keys
chown username /home/username/.ssh/authorized_keys
chmod 600 /home/username/.ssh/authorized_keys
```

- 3) For each administrator, generate a public/private key pair on the administrator's SSH client.
- 4) Add each administrator's public key to their `authorized_keys` file on the firewall.
 - a) In the Admin Console, select **Maintenance > File Editor**, then click **Start File Editor**. The File Editor window appears.
 - b) Select **File | Open**. The **File Editor: Open File** window appears.
 - c) Select **Firewall File**.
 - d) In the **File** field, type `/home/username/.ssh/authorized_keys`.
 - e) Click **OK**. The `authorized_keys` file opens.

- f) Paste the contents of the administrator's public key into the File Editor, then save your changes and close the File Editor.
- 5) [Conditional] If necessary, enable or modify the **Secure Shell Server** rule.

Related tasks

[Manage SSH access](#) on page 568

Configure SSH-2 public key authentication for the firewall SSH client

To use the firewall as an SSH client with RSA, DSA, or ECDSA authentication, you must perform several configuration steps before initiating the SSH connection.

Steps

- 1) For each administrator, generate a public/private key pair.
 - a) Connect to the firewall using the Admin Console, and log on as the administrator you are generating a client key for.
 - b) Select **Maintenance > Remote Access Management**, then click the **SSH Server Properties** tab.

Tip: For option descriptions, click **Help**.
 - c) Click **Generate new client keys**.
 - If a warning pop-up window appears, click **Yes** to replace the existing keys or **No** to cancel.
 - If a message appears indicating new keys have been installed, click **OK**.
- 2) Export the public key for each administrator to the corresponding .ssh directory on the destination SSH server(s).
 - If the destination SSH server is another Sidewinder, export the public key file using the Admin Console.
 - If the destination SSH server is not a Sidewinder, manually transfer the public key.

Related tasks

[Export an administrator's public key to another Sidewinder](#) on page 573

[Export an administrator's public key to an SSH server](#) on page 573

Export an administrator's public key to another Sidewinder

Use the Admin Console to export an administrator's public key to another firewall by connecting to both firewalls.

Steps

- 1) In the Admin Console, connect to the source firewall and the destination firewall.
- 2) For the source firewall, select **Maintenance > Remote Access Management**, then click the **SSH Server Properties** tab.



Tip: For option descriptions, click **Help**.

- 3) Click **Export client keys**. The **SSH Server Properties: Export Client Key** window appears.
- 4) Select the destination firewall, then click **OK**. When the export is complete, a pop-up window appears. Click **OK** to close the pop-up window.

Export an administrator's public key to an SSH server

To export an administrator's client key to an SSH server, you must manually transfer the file.



CAUTION: Never transfer the private key.

Transfer the public key using one of the following methods:

- **Copy and paste** — Open the public key file in the Admin Console File Editor and paste its contents into a new file.
- **File transfer** — Transfer the public key file using a secure method such as SFTP.



CAUTION: Do not use FTP or another protocol that is not secure to transfer the public key.

Related concepts

[Configuring SSH-2 public key authentication for SSH](#) on page 570

Local management

You can access the command line interface by logging directly on to the firewall.

Local access can be provided using the following methods:

- Monitor and keyboard
- Terminal or terminal emulator connected to the serial port

Log on locally

Log on to the firewall at the local console.

Steps

- 1) At the login prompt, type your user name and press **Enter**. The Password prompt appears.
- 2) Type your password and press **Enter**. The User domain prompt appears:

```
firewall_name:User {1} %
```

When you initially log on at the command line interface, you are logged on to the User domain, which allows limited access.
- 3) To change to the Admn domain, which allows access to all firewall domains (based on your administrative role), enter the command:

```
srole
```
- 4) To return to the previous domain role and shell, enter the command:

```
exit
```


You are returned to the User domain.

Manage local access

Local access is controlled using an access control rule. To enable or disable local access, modify the **Login Console** rule.

Steps

- 1) Select **Policy > Access Control Rules**
- 2) Expand the **Administration** rule group.



Tip: For option descriptions, click **Help**.
- 3) Select the **Login Console** rule, then select **Enable** or **Disable** as necessary.
- 4) Save your changes.

General maintenance

Contents

- [Manage administrator accounts](#) on page 575
- [Understanding time synchronization](#) on page 578
- [Configure time synchronization](#) on page 581
- [Configure network clocks](#) on page 583
- [Configure firewall self-diagnostics](#) on page 584
- [Enable hardware acceleration](#) on page 586
- [Understanding software management](#) on page 586
- [Update software](#) on page 588
- [Shutdown options](#) on page 596
- [Configure the firewall for UPS](#) on page 598
- [Register the firewall with Control Center](#) on page 599
- [Manage service updates](#) on page 600
- [Editing files](#) on page 601
- [Backing up and restoring the firewall configuration](#) on page 606
- [Make the firewall FIPS 140-2 compliant](#) on page 616

Keep your firewall operating effectively by setting the date and time and keeping the software up to date.

Manage administrator accounts

Each Sidewinder administrator must have an account on the firewall. The initial administrator account is created during the Quick Start Wizard configuration.



Note: Only administrators have accounts directly on the firewall. Users of firewall networking services have user (or network logon) accounts.

When you add an administrator account, you also assign the new administrator a role.

The following table describes the available administrator roles.

Table 101: Administrator roles

Role	Authorized to:
admin	<ul style="list-style-type: none"> • Access all windows, menus, and commands within the Admin Console. • Add and remove users and assign roles. • Do incremental back-ups and restore the system. • Use all other system functions and commands.

Role	Authorized to:
adminro	This role allows an administrator to view all system information, as well as create and run audit reports. An administrator with read-only privileges cannot commit changes to any area of the firewall. In the Admin Console, restricted options are unavailable, grayed out, or Modify buttons are replaced with View .
no admin privileges	Maintains an existing or new administrator account with limited access to the User domain. This role is generally used to temporarily disable an administrator account.

Related concepts

[Users and user groups](#) on page 106

Create an administrator account

Create a new administrator account.

Steps

- 1) Select **Maintenance > Administrator Accounts**. The **Administrator Accounts** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **New**. The **New Administrator** window appears.
- 3) Complete the information, including the admin role.
Consider the following regarding the **Username** field:
 - The name must be between 1–16 alphanumeric characters.
 - Do not use uppercase characters. Sendmail automatically converts the user name to lowercase before delivering email; email addressed to a user name containing uppercase characters is not forwarded.
 - Once you create the account, the name cannot be modified.
- 4) Click **Add**. The administrator account appears.

Related reference

[Administrator information](#) on page 35

Modify an administrator account

Change an existing administrator account.

Steps

- 1) Select **Maintenance > Administrator Accounts**. The **Administrator Accounts** window appears.



Tip: For option descriptions, click **Help**.

- 2) Select the administrator account you want to change, then click **Modify**. The **Modify Administrator** window appears.
- 3) Make your changes, then click **OK**.

Delete an administrator account

Delete an existing administrator account.

Steps

- 1) Select **Maintenance > Administrator Accounts**. The **Administrator Accounts** window appears.



Tip: For option descriptions, click **Help**.

- 2) Select the administrator account you want to delete, then click **Delete**. The confirmation window appears.
- 3) Click **Yes** to delete the administrator account or **No** to cancel the action.

Change the administrator password

Change the password (UNIX account password) on an administrator account.

Steps

- 1) Select **Maintenance > Administrator Accounts**. The **Administrator Accounts** window appears.



Tip: For option descriptions, click **Help**.

- 2) Select the administrator account you want to change the password for, then click **Modify**. The **Modify Administrator** window appears.
- 3) In the **Password** field, highlight the existing password and type the new password.
- 4) In the **Confirm** password field, retype the password.

- 5) Click **OK**.

Related tasks

[Change password \(forgot\)](#) on page 676

Understanding time synchronization

Network Time Protocol (NTP) allows you to synchronize all clocks on a network or synchronize the clocks on one network with those on another network.

Using NTP with the firewall provides these benefits:

- Time is set accurately.
- Synchronized network systems are useful for audit logs.
- The external time source is more accurate when synchronizing your network for time-critical services.
- High Availability clusters benefit from synchronized time.

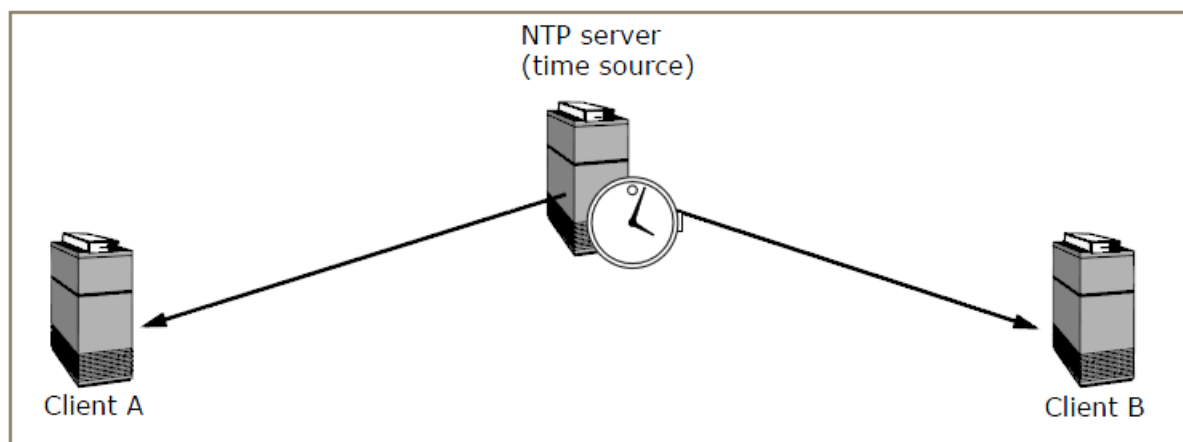
Sidewinder is compatible with NTP versions 2, 3, and 4. Version 4 is the preferred version and is the firewall default.

NTP servers and clients

In NTP, a server is a system that sends a time feed to another system. (The server is also referred to as a host.) The receiving system—the one whose time is being set by the server—is an NTP client. The firewall can be set up as an NTP server or a client.

The figure shows a simple configuration with an NTP time server and two NTP clients (A and B) in the same network. The NTP server supplies the time to NTP clients A and B. Using their own NTP software, each client system must also be set up to receive time from the server.

Figure 75: NTP server-client relationship

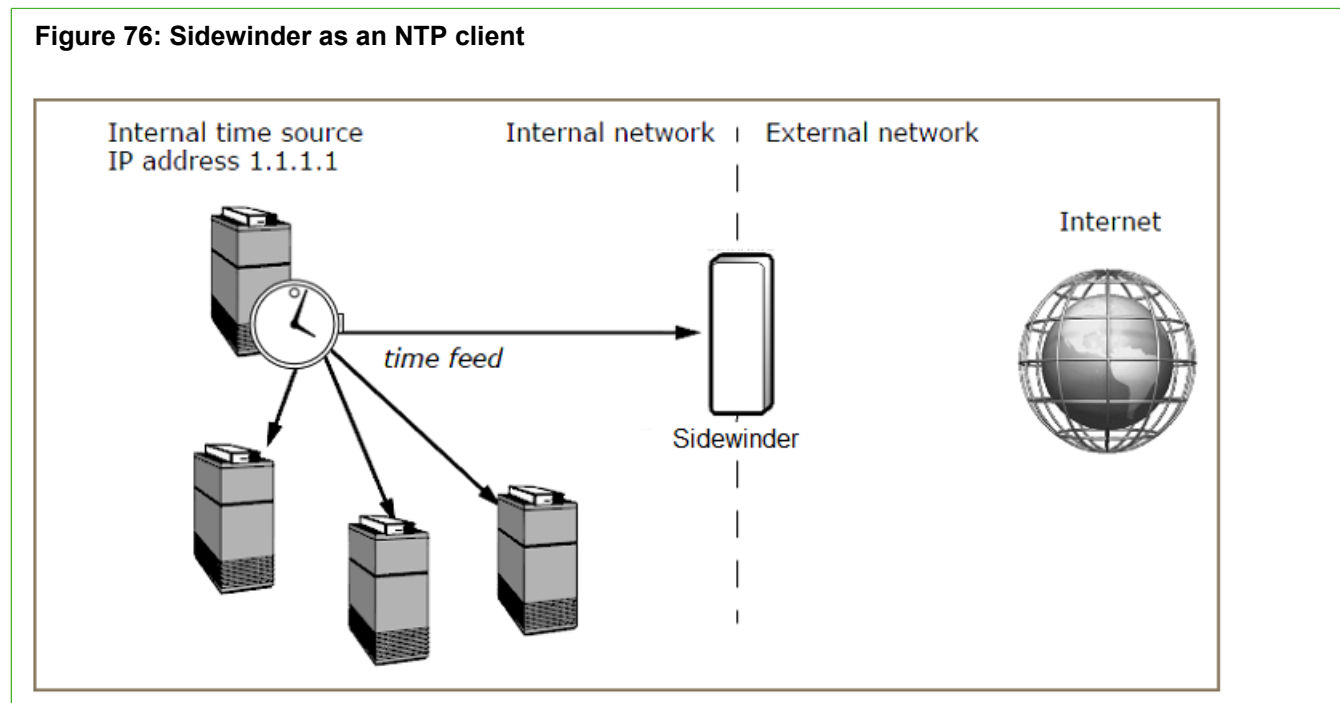


Sidewinder as NTP client

It is the recommended configuration with the firewall configured as a client receiving time from a server (Internal time source).

Refer to the figure for an illustration of a common NTP setup. In this configuration, a server in the internal network (shown with an analog clock) is the designated time-setter for the rest of the network. The other three systems in the internal network are also NTP clients.

Figure 76: Sidewinder as an NTP client



The internal server provides time to the firewall and to other internal computers. There is no time feed to or from the Internet.

By means of NTP, the server automatically maintains the correct time on the firewall and also maintains the time on other computers in the network.

The internal network does not rely on an external time server, so it is not exposed to any security breaches that could result. Since the firewall is not supplying time for other systems but is only receiving it, this setup has a minimal effect on firewall performance.



Note: Do not configure the firewall to receive time from both an internal and external NTP server. The firewall should receive time on only one zone. Input from the external time server cannot be reconciled with that from the internal server.

Sidewinder as NTP server

You can also set up the Sidewinder to be a time-setter for the rest of the network. The firewall can receive time from an external NTP server, then feed the time to an internal system, which in turn supplies time to your other computers.

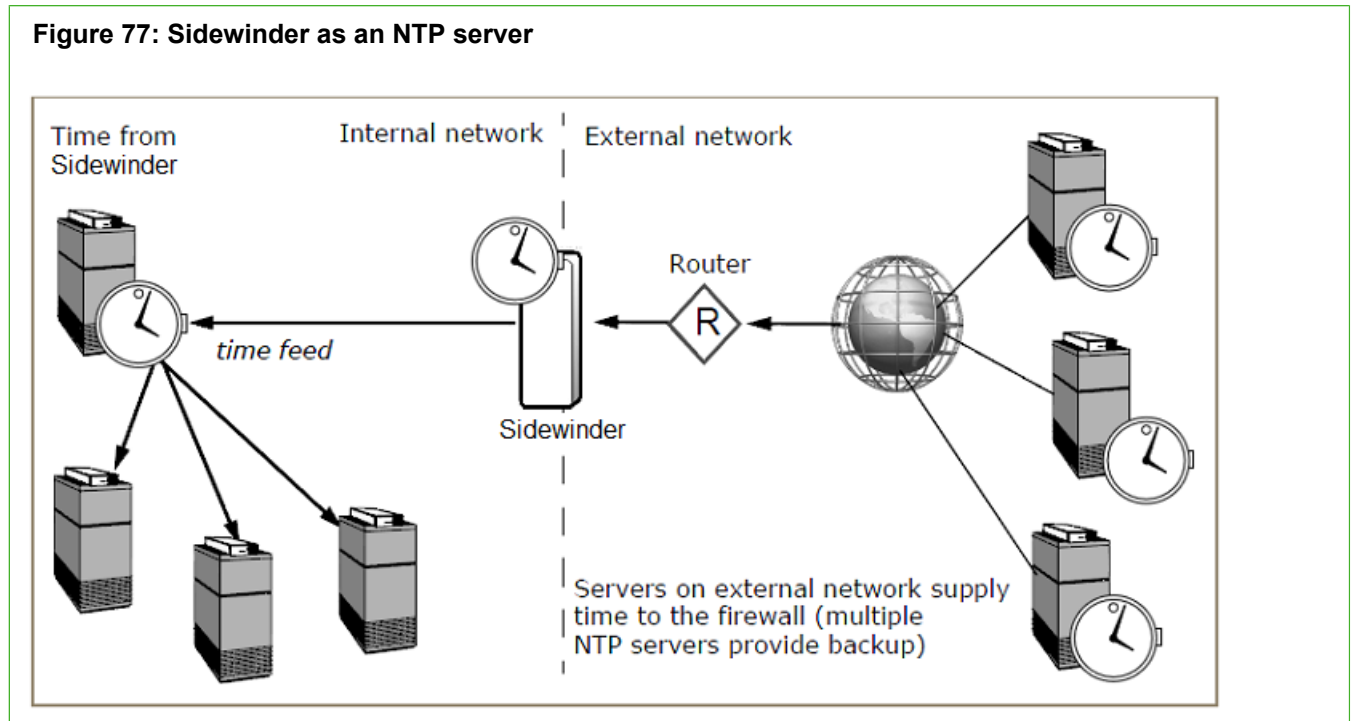
- Serving time directly from a Sidewinder to several clients can slow the performance of the firewall.
- If the firewall is serving time (host), its clients should not receive time from any other NTP server.

In the figure, the firewall is receiving time from NTP servers on an external network and passing the time on to the internal network. This would be advantageous if your company required constant and precise time updates to within microseconds of world standard time. In this scenario, the router must be able to handle NTP traffic.



Note: An external-to-internal NTP configuration might introduce security concerns to the firewall and thus to your network. Therefore, this configuration is only recommended for sites that need world standard time.

Figure 77: Sidewinder as an NTP server



External time servers supply time to the firewall, which passes time to the internal system.

References for NTP

NTP is a complicated protocol with many options. There are numerous places where more information can be obtained. These include RFCs, websites, and local manual (man) pages.

For more information about NTP, see the following sources:

Internet Request For Comments (RFC)

The following RFCs provide information on NTP:

- RFC 1119 Network Time Protocol (Version 2)
- RFC 1305 Network Time Protocol (Version 3)
- RFC 4330 Simple Network Time Protocol (Version 4)

Websites

Visit <http://www.ntp.org/>.

On-line manual (man) pages

Type the following commands:

```
man cf_ntp
```

```
man ntpd  
man ntpdc  
man ntpdate
```

Configure time synchronization

Enable NTP on the firewall.



Tip: For best results, set the firewall time as close as possible to the NTP server time. If the times are too far apart, it could take a long time for the NTP server to synchronize with the firewall.

Configure Sidewinder as an NTP client

Configure the firewall as an NTP client for an internal NTP server.



Tip: For best results, set the firewall time as close as possible to the NTP server time. If the times are too far apart, it could take a long time for the NTP server to synchronize with the firewall.

Steps

1) Select **Maintenance > Date and Time**. The **Date and Time** window appears.



Tip: For option descriptions, click **Help**.

2) In the **Enable Network Time Protocol (NTP) on** pane, select the firewall zone that receives time updates from the NTP server.

3) Add one or more NTP servers.

a) In the **NTP Servers** pane, click **New**. The **New NTP Server** window appears.

b) In the **Server** field, type the IP address or host name of the NTP server.

c) From the **Zone** drop-down list, select the zone that communicates with the NTP server. This enables the NTP service in the appropriate zone.

d) [Optional] If you want this to be the preferred NTP server, select the **Preferred Server** checkbox.

e) Click **Add**.

Result

The server appears in the **NTP Servers** pane.

Configure Sidewinder as an NTP server

Configure the firewall to receive time from an NTP server and serve time to clients.

Steps

- 1) Select **Maintenance > Date and Time**. The **Date and Time** window appears.



Tip: For option descriptions, click **Help**.

- 2) In the **Enable Network Time Protocol (NTP)** on pane, enable the NTP service in the appropriate zones.
 - One zone communicates with external NTP servers.
 - One zone feeds time to the internal time server.

- 3) Add one or more external NTP servers.

- a) In the **NTP Servers** area, click **New**. The **New NTP Server** window appears.
- b) In the **Server** field, type the IP address or host name of the external NTP server.
- c) From the **Zone** drop-down list, select the external Sidewinder zone that communicates with the NTP server.
- d) [Optional] If you want this to be the preferred NTP server, select the **Preferred Server** checkbox.
- e) Click **Add**.

- 4) Add Sidewinder as a time server.

- a) In the **NTP Servers** pane, click **New**. The **New NTP Server** window appears.
- b) Type the following IP address: `127.127.1.0`
This signals the firewall to use the local hardware clock as its time source.



Note: If you do not configure a remote time source, this clock address is taken as default for 8.1.1 and later.

- c) From the **Zone** drop-down list, select the Sidewinder zone that communicates with the internal time server.
- d) [Optional] If you want this to be the preferred NTP server, select the **Preferred Server** checkbox.
- e) Click **Add**.

Modify an NTP server

Change the IP address, zone, or preferred server setting for an NTP server.

Steps

- 1) Select **Maintenance > Date and Time**. The **Date and Time** window appears.



Tip: For option descriptions, click **Help**.

- 2) Select the server you want to modify, then click **Modify**.
- 3) Make your changes, then click **OK**.

Delete an NTP server

Delete an NTP server that you no longer want the firewall to pull time from.

Steps

- 1) Select **Maintenance > Date and Time**. The **Date and Time** window appears.



Tip: For option descriptions, click **Help**.

- 2) Select the server you want to delete, then click **Delete**. The confirmation window appears.
- 3) Click **Yes** to delete the NTP server or **No** to cancel the action.

Configure network clocks

Use the Admin Console to set the time zone, date, and current time for the firewall.



Note: When you change these settings, the firewall automatically restarts. We recommend modifying these settings during off-hours.

Set the time zone

Setting the correct time zone is important for accuracy in your audit logs.



Note: When you change these settings, the firewall automatically restarts. We recommend modifying these settings during off-hours.

Steps

- 1) Select **Maintenance > Date and Time**. The **Date and Time** window appears.



Tip: For option descriptions, click **Help**.

- 2) [Conditional] If you want to use Greenwich Mean Time (GMT)—also known as Coordinated Universal Time (UTC)—select **Use GMT (UTC)**.
- 3) In the **Region** field, use the drop-down list to select the region where the firewall is located.
- 4) In the **Country** field, use the drop-down list to select the country where the firewall is located.
- 5) In the **Zone** field, use the drop-down list to select the time zone where the firewall is located.

Set the date and time

Setting the correct date and time is important for accuracy in your audit logs.



Note: When you change these settings, the firewall automatically restarts. We recommend modifying these settings during off-hours.

Steps

- 1) Select **Maintenance > Date and Time**. The **Date and Time** window appears.



Tip: For option descriptions, click **Help**.

- 2) In the **Date** field, use the drop-down list to access the calendar. Use the left and right arrows to select a month, then select a date.
- 3) In the **Time** field, select and replace the time, or use the up and down arrows to refine the time.

Configure firewall self-diagnostics

You can configure the firewall to respond to processes that monopolize the CPU, such as hot processes.

The monitor daemon can be configured to identify hot processes. The firewall can generate audit, send alerts, or terminate hot processes. Self-diagnostics are configurable from the command line interface.



Note: If processes are identified as hot processes, only daemond-managed processes can be terminated.

Setting up diagnostic responses before a hot process occurs offers the opportunity to gather data and avoid the need to re-create the event that caused the hot process. The diagnostic data can be shared with [Forcepoint support](#) to resolve the issue. Another benefit is that administrators are notified when hot processes occur and can respond in a timely manner. The diagnostic files are stored in `/var/diagnostic/`.

Steps

- 1) From the command line, log on and enter `srole`.
- 2) Enter the `monitord` command.
For example, `cf monitord set hot_process_audit_duration=2` alerts the administrator after a process has run hot for two minutes.

Table 102: Self-diagnostic commands and functions

Command fragment	Setting options	Purpose
<code>cf monitord set</code>	Must be combined with an action key.	Sets monitord options.
Action keys		
<code>hot_process_threshold=90</code>	Allowed range is from 80 to 100%. The default setting is 90%. Recommended range is between 90 to 100%.	CPU usage threshold for processes. If CPU usage of a process reaches this value, it will be considered as a hot process.
<code>hot_process_audit=on</code>	On or off. This setting is enabled by default.	When enabled, monitord will generate audit or alert user when a process goes hot over the configured <code>hot_process_audit_duration</code> .
<code>hot_process_audit_duration=5</code>	Number of minutes. The default setting is 5 minutes.	Duration to wait before alerting the administrator about the hot process.
<code>hot_process_diagnostic=off</code>	On or off. This setting is off by default.	When enabled, monitord will terminate the hot process and generate diagnostic when the process continues to be hot over the configured <code>hot_process_diagnostic_duration</code> .
<code>hot_process_diagnostic_duration=30</code>	Number of minutes. The default setting is 30 minutes.	Duration to wait before terminating the hot process and generating diagnostic.

- 3) Run the `cf monitord query` command to confirm your settings.
- 4) [Optional] Modify the default **System Response** for hot processes.

Result

For instructions on submitting your files to [Forcepoint support](#), see the *Forcepoint Sidewinder Command Line Interface Reference Guide*.

Related tasks

[Create a system response](#) on page 326

Enable hardware acceleration

If you use SSL decryption, you can use a supported hardware accelerator card in your firewall to offload decryption, increasing system performance.



Note: If you do not have a supported hardware accelerator card installed on your firewall and would like to use one, contact your sales representative for assistance. To install a hardware accelerator card, consult the product documentation for the accelerator and chassis.

Steps

- 1) To enable a hardware accelerator card, select **Maintenance > Hardware Acceleration**. The **Hardware Acceleration** window appears and displays information about the hardware acceleration card installed on your firewall.



Tip: For option descriptions, click **Help**.

- 2) To implement these changes, select **Maintenance > System Shutdown**, and restart the firewall.



Note: You must restart the firewall whenever you enable or disable a hardware accelerator card.

Understanding software management

Updates can include improvements and enhancements to the Sidewinder software as well as updates to optional features.

The types of software updates are:

- **Major** — A major release with significant enhancements and added functionality. Example: 8.0.0.
- **Minor** — A minor release with new features. Example: 8.1.0, 8.2.0.
- **Maintenance** — Released periodically and contains software fixes; maintenance releases must be installed sequentially. Example: 8.0.1, 8.2.1.
- **Speciality** — These releases vary depending on the requirements.
 - **Vendor** — Contains fixes, updates, or new features specific to a particular component, for example anti-virus add-on module. Example: 8.0.0MCV01.



Note: Only install the patch if you have the feature enabled. Install patches sequentially.

- **Upgrade** — Brings your firewall to a new major or minor version. Example: 701UP, 8.0.0UP.
- **Patch** — Contains an issue-specific fix and should be installed only if it addresses a current problem. Example: 8.0.0P01, 8.0.0P02.
- **E-Patch** — Sent to a particular customer on an as-needed basis to determine if the fix corrects an identified defect for a particular version of the product. If the fix works, it is then converted to a patch or incorporated into a future major, minor, or maintenance product release. Example: 8.0.0E01, 8.0.0E02.
- **Restricted** — Restricted distribution to identified customers to solve a particular defect. Example: 8.0.0R01, 8.0.0R02.
- **Hardware** — A limited-distribution update required to support new hardware. Example: 8.0.0HW01.

Related concepts

[Loading and installing](#) on page 587

[Uninstalling and rolling back](#) on page 587

[Re-installing and re-imaging](#) on page 588

Loading and installing

Periodic software updates, called *packages*, are available on our FTP site.

- **Load** — You load a package onto the firewall. This moves the package from the FTP site to the firewall, but does not install it.
 - Packages can be loaded manually, at automatic intervals, or at scheduled times using the Manage Packages and Download Packages tabs.
 - The FTP site is the default location for software packages. You might configure a different location to load packages from if you have firewalls on an isolated network, or to speed up downloads to several firewalls.
- **Install** — Packages that are loaded on the firewall can then be installed on the firewall using the Manage Packages tab.
 - Packages can be installed manually or automatically at a scheduled time. Packages can be installed individually or several at a time.
 - Key package information is provided, such as dependencies with other packages, whether a restart is required, and whether the package can be uninstalled.

Uninstalling and rolling back

If you are not satisfied with an update, you can uninstall the package or revert to the previous configuration.

- **Uninstall** — Package uninstalls are performed on the **Manage Packages** tab.
 - The **Uninstallable** column states if a package is uninstalleable.
 - Any configuration changes you make after the package was installed remain after the package is uninstalled.
 - Packages can be uninstalled manually or automatically at a scheduled time. Packages can be uninstalled individually or several at a time.
 - Uninstalled packages remain loaded on the firewall.
- **Rollback** — Use the **Rollback** tab to restore the firewall to a previous state. Rolling back is an option if a package is not uninstalleable.

- Any configuration changes made after the package was installed are lost. A rollback reverts the firewall to the state just before the package was installed. Therefore, rolling back is a recommended recovery option for only a short time after a package installation.
- A rollback can be performed manually or automatically at a scheduled time.
- A rollback always requires a restart.
- The tab displays what patch level the firewall will roll back to and the date and time the patch was loaded.

Re-installing and re-imaging

Serious issues might require you to re-install or re-image your Sidewinder.

- **Re-install from the virtual CD** — Use the virtual CD function to re-install the Sidewinder software. Re-installing from the virtual CD puts the firewall in its original unconfigured state.
- **Re-install using the installation media** — For instructions on re-imaging a firewall using the installation media, refer to the *Forcepoint Sidewinder Release Notes*.

Related tasks

[Manage software packages](#) on page 588

[Download Packages](#) on page 592

[Rollback the firewall](#) on page 594

[Re-install your firewall from the virtual CD](#) on page 700

Update software

The firewall comes installed with the latest software available at the time. Use the **Software Management** window to keep your firewall current with updates.

You can also uninstall updates or revert to a previous configuration.

Manage software packages

Manage software packages for Sidewinder from the **Software Management** window.

Select **Maintenance > Software Management**. The **Software Management** window appears with the **Manage Packages** tab open.



Tip: For option descriptions, click **Help**.

You can perform the following tasks.

View available packages

Available packages appear when they are loaded from a site. They are not yet installed.

To populate the table with packages that are available for downloading, click **Check for Updates**. Packages appear in the table with a status of *Available*.

Available packages are loaded from our FTP site, or from another site you designate on the **Download Packages** tab.

Use the **Download Packages** tab to configure automatic checking and loading, and to change the location where packages are downloaded from.

Sort the Manage Packages table

Select and sort the package types from the table of packages.

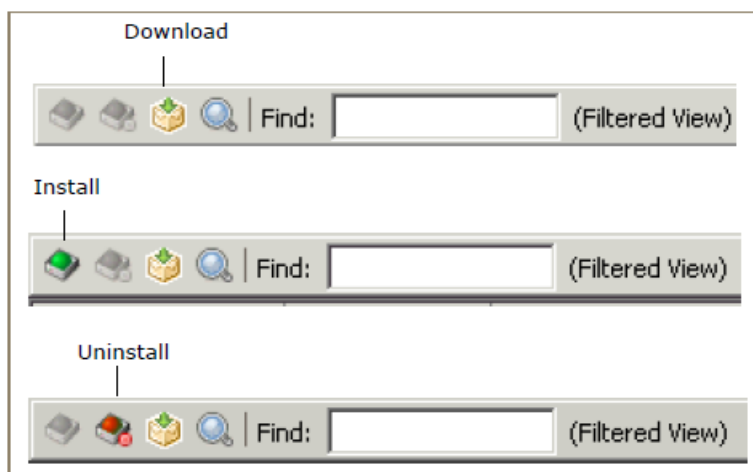
- Select which package types and statuses appear in the table: Click **View Options** and make your selections in the pop-up window.
- Sort the **Package Name** column in ascending or descending order by clicking the column heading.
- Sort other columns by right-clicking a column heading and selecting a filter option from the pop-up list.
- Use the **Find** field to search for a specific element(s) in the list. Type your search criteria, and only packages with matching elements will appear in the list.

Load, install, and uninstall packages now

Use the **Manage Packages** table to load, install, or uninstall packages immediately.

- The buttons that appear depend on the status of the package selected in the table:

Figure 78: Manage Packages table buttons



- You can select more than one package to manage.
 - The packages you select must have the same status.
 - Select several consecutive packages by selecting the first package, then pressing the **Shift** key while selecting the last package. To select several non-consecutive packages, press the **Ctrl** key as you select each desired package.

Download a package to Sidewinder

Download a package to the firewall for installation.

Steps

- 1) Select a package in the table with the status of *Available*.



Tip: For option descriptions, click **Help**.

- 2) Click **Download**. A "successfully loaded" message appears and the package status changes to *Loaded*.

Install a package

Perform these steps to install a software package.

Steps

- 1) Select a package in the table with the status of *Loaded*.



Tip: For option descriptions, click **Help**.

- 2) Click **Install**. The **Install** window appears.

If the package has dependencies, the dependencies appear in a lower table.

- If a dependency is loaded, it is installed at the same time as the selected package. If you do not want to install the dependency, click **Cancel**. The selected package and dependency will not be installed.
- If a dependency is not loaded, a message states that you must load the dependency before installing the selected package. Click **Cancel** to exit the Install window.



CAUTION: If you install multiple packages and one of the installations fails, the firewall will not restart and a successful installation that requires a restart will not be complete. You must investigate the cause of the installation failure and determine if you should manually restart the firewall or uninstall the package.

- 3) Select **Install now**.
- 4) [Conditional] If the package requires a restart, select whether you want the restart to occur after installation.
 - If you select **Activate packages after installation**, the package is installed, the firewall restarts, and the package is activated after you click **OK**.
 - If you clear **Activate packages after installation**, the package is installed after you click **OK** but the firewall does not restart and the package is not activated. A rollback is required to activate the package after installation. You will be prompted to schedule a rollback to activate the package.
- 5) Click **OK**.

Result

The package appears in the **Manage Packages** table with a status of *Installed*.

Uninstall a package

Select and uninstall a package from the table.

Steps

- 1) Select a package in the table with the status of *Installed*.



Tip: For option descriptions, click **Help**.

- 2) Click **Uninstall**. The **Uninstall** window appears.
If the package has a dependency, the dependency appears in a lower table and will be uninstalled at the same time as the selected package. If you do not want to uninstall the dependency, click **Cancel**. The selected package and dependency will not be uninstalled.
- 3) Select **Uninstall now**, then click **OK**.

Result

The package appears in the **Manage Packages** table with a status of *Loaded*.

Schedule automatic installs and uninstalls

Schedule a time to install or uninstall packages.

Steps

- 1) On the **Manage Packages** tab, click **Schedule**. The **Schedule Install/Uninstall** window appears.
 - Any package with a status of *Loaded* appears in the **Select packages to install** list.
 - Any package with a status of *Installed* appears in the **Select packages to uninstall** list. (If a package cannot be uninstalled, it does not appear in the list.)



Tip: For option descriptions, click **Help**.


- 2) Select the packages you want to install or uninstall.
- 3) Select **Schedule for** and select a date and time for the action to take place.
- 4) Click **OK**.

The selected packages appears in the **Manage Packages** table with a status of *Install scheduled on <date>* or *Uninstall scheduled on <date>*.

To cancel a scheduled install or uninstall, select **Unschedule All** and click **OK**.

View package information and activity logs

You can view information and activity for all packages listed in the **Manage Packages** table.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) View information and activity logs for a single package.
 - a) In the **Manage Packages** table, select a package.
 - b) Click **View Package Details**
 - The **Readme** tab states what changes the package is making.
 - The **Package Log** tab shows all load, install, and uninstall activities for the package.
- 2) View all package installation activities on this firewall.
 - a) Click **View Log**. The **View Log** window appears.
 - b) The **View Log** lists detailed histories of all package installs and uninstalls on the firewall, including programs run, package parameters, and errors.

Enable email notification

Enable e-mail notification of software management activities.

Steps

- 1) Select **Enable e-mail notifications for install, uninstall, automatic load and rollback**.



Tip: For option descriptions, click **Help**.

- 2) In the **E-mail Address** field, enter the e-mail address of the person who will be notified. The default address is the administrator of this firewall.
- 3) Save your changes.

Download Packages

Manually or automatically load software packages onto the firewall.

Select **Maintenance > Software Management**, then click the **Download Packages** tab. The **Download Packages** window appears.



Tip: For option descriptions, click **Help**.

To configure your firewall to load packages automatically:

Steps

- 1) Select an automatic action:
 - **Automatically check for and load packages** — To find available packages and load them on the firewall, select this option. Packages appear in the **Manage Packages** table with a status of *Loaded*. They can be installed.
This option works well if you regularly schedule package installations.
 - **Automatically check for available packages** — To find available packages, select this option. A list of packages appears in the **Manage Packages** table with a status of *Available*. They can be loaded.
This option works well if downloading to your firewall is slow, or if you do not want to store and manage packages you will not use.
- 2) Identify the package site:
 - **Load using** — Select the protocol used to transport the package.
 - **Directory** — The path name on the site where the package is located.
 - **Host** — The host name or IP address of the site where the package is located.
 - **User Name** — The user account defined on the site.
 - **Port** — The number of the port used to access the site.
 - **Password** — The password to validate you to the site.
 - **Confirm Password** — Verify the password.



Note: To restore the system default values to these fields, click **Restore Defaults**.

- 3) From the **Frequency** drop-down list, select how often you want the firewall to check for available packages.



Note: Use `cf crontab` to designate a specific time for the action to take place. See the *Forcepoint Sidewinder Command Line Interface Reference Guide*.

- 4) Save your changes.

Result

To manually load a package:

- 1) Click **Perform Manual Load Now**. The **Download Packages: Manual Load** window appears.
- 2) Identify the package and its location:
 - **Load packages from** — Select the location of the package you are loading to the firewall. It can be an FTP or HTTPS site, a CD-ROM, or a file.
 - **Directory** — The path name where the package is stored.
 - **Packages** — The name of the package you are loading. If you are loading more than one package, separate each package name with a comma. Package names contain only alphanumeric characters. No spaces are allowed in package names.
 - **Host** — [Conditional] The host name of the FTP or HTTPS site where the package is located.
 - **User Name** — [Conditional] The user account defined on the FTP or HTTPS site.
 - **Port** — [Conditional] The number of the port used to access the FTP or HTTPS site.
 - **Password** — [Conditional] The password to authenticate to the FTP or HTTPS site.
 - **Confirm Password** — [Conditional] Verify the password.

- 3) Click **OK**. Click **Yes** to confirm the load. The package appears in the **Manage Packages** tab with a status of *Loaded*. The package can be installed.

Rollback the firewall

You can roll back the firewall to a previous state.

The table shows which packages will be on the firewall after the rollback.

- Any configuration changes made after the last package was installed are lost. A rollback reverts the firewall to the state just before the package was installed. Therefore, rolling back is a recommended recovery option for only a short time after a package installation.
- A rollback requires a restart.

Steps

- 1) Select **Maintenance > Software Management**, then click the **Rollback** tab.

The **Rollback** window appears.



Tip: For option descriptions, click **Help**.

- 2) Click **Rollback Now**. A warning message appears stating that configuration changes will be lost and that the firewall will restart.
- 3) Click **Yes** to continue. The firewall restarts.
To schedule the rollback for a future time:
 - a) Select **Schedule rollback for** and select the desired date and time.
 - b) Save your changes. A warning message appears stating that configuration changes will be lost.
 - c) Click **Yes** to schedule the rollback.

Upgrade a firewall

Select the appropriate upgrade method for your firewall type.

Before you begin

- Your firewall must be at the previous version.
- [Virtual appliances only] Your system must support Intel VT technology (or equivalent). Verify that VT is enabled in your computer BIOS.

Upgrade a standalone firewall or HA cluster

Use the Admin Console to upgrade a standalone firewall or HA cluster with these high-level steps.



Note: To upgrade an HA cluster, upgrade the secondary/standby firewall first, then upgrade the primary firewall. Once both cluster members are upgraded, the policy synchronizes.

- 1) Create a configuration backup.
- 2) Download the package.
- 3) Install the package.

Related tasks

[Back up configuration files](#) on page 606

[Download Packages](#) on page 592

[Install a package](#) on page 590

[Rollback the firewall](#) on page 594

Upgrade a Control Center-managed firewall or HA cluster

Use Control Center to upgrade managed firewalls and clusters.



CAUTION: Do not use the Sidewinder Admin Console to install a patch directly on a managed firewall.

Steps

- 1) Upgrade your Control Center; see the *Forcepoint Sidewinder Control Center Release Notes*.
- 2) Use Control Center to upgrade the managed firewall to the new version; see the *Forcepoint Sidewinder Control Center Product Guide*.

Shutdown options

There are four Sidewinder shutdown options.

- Restart to Operational Kernel
 - The firewall boots to the Operational kernel by default. You can boot to the Operational kernel through the Admin Console or by pressing the power button.
 - You can log on to the firewall using the Admin Console and perform administrative tasks.
- Shutdown to Emergency Maintenance Mode
 - Emergency Maintenance Mode (EMM) allows you to do repair work with other services turned off. You should use EMM only if directed by [Forcepoint support](#).
 - The # prompt appears on the firewall, indicating that you are in a login shell and can start issuing firewall or UNIX commands.
 - The firewall in EMM is offline and does not pass traffic.
 - You must connect a console to the firewall in order to work with it. You cannot access the firewall via the Admin Console, SSH, or telnet in emergency maintenance mode.
- Halt System
 - The operating system shuts down, but the system remains powered on.
 - Halt System is useful if you need to connect directly to the firewall to access the BIOS.
- Power Down System
 - You completely shut down the firewall without restarting.
 - Power down the system before you move your firewall to a new location or make hardware changes.

You can restart or shut down a firewall from the Admin Console or the command line.

- When the firewall restarts or is shut down, a record of who issued the action is logged in the `/var/log/messages` file. This applies to a restart or shutdown issued from the Admin Console or using the `shutdown` command.
- If the boot process fails, contact [Forcepoint support](#).

Restart or shut down using the Admin Console

Perform these steps to restart the firewall or to shut down the firewall completely.

Steps

- 1) Select **Maintenance > System Shutdown**.

The **System Shutdown** window appears.



Tip: For option descriptions, click **Help**.

- 2) In the **Shutdown Options** area, select the action you want to perform:
 - **Restart to Operational Kernel** — Restarts the system in the Operational kernel.
 - **Shutdown to Emergency Maintenance Mode** — Restarts the system in emergency maintenance mode and displays the # prompt, indicating that you are in a login shell and can start issuing firewall or UNIX commands.
 - While the firewall is in emergency maintenance mode, it is offline and does not pass traffic.

- You must connect a console to the firewall before you can administer the system in emergency maintenance mode.
 - **Halt System** — Shuts down the operating system, but the system remains powered on. Run this command if you need to connect directly to the firewall to access the BIOS.
 - **Power Down System** — Completely shuts down the firewall software without restarting. Run this command before you move your firewall to a new location or make hardware changes.
- 3) [Optional] If you want a shutdown message to appear informing users of a pending shutdown, type the message text in the **Shutdown Message** field.
 - 4) In the **Shutdown Time** field, select the shutdown time from the following options.
 - **Shutdown Immediately** — The system will shut down immediately when you click **Perform Shutdown**.
 - **Delay Shutdown for** — The shutdown will be delayed for the amount of time specified in the **Hours** and **Minutes** fields. You can enter values in these fields that will delay the shutdown for up to 24 hours and 59 minutes.
 - 5) Click **Perform Shutdown** to implement the shutdown.
 Any connections to the Admin Console will be lost when the firewall shuts down. New connections to the firewall will not be allowed once the shutdown process has been executed.

Restart or shut down using a command line interface


The `shutdown` command restarts or shuts down the system from a command line interface. Use this command to indicate how and when you want the firewall to shut down.

The table below shows some common shutdown commands from the command line.

More information about shutdown options is available on the `shutdown` man page.

Table 103: Shutdown commands on the command line

Command	Type of shutdown
<code>shutdown -r [time]</code>	Restarts the system in the Operational kernel. For example, <code>shutdown -r +120</code> would restart the firewall into its Operational kernel in two hours (120 minutes).
<code>shutdown [time]</code>	Restarts the system to emergency maintenance mode. For example, <code>shutdown now</code> would immediately restart the firewall into emergency maintenance mode.
<code>shutdown -h [time]</code>	Shuts down the firewall without restarting. For example, <code>shutdown -h 0601312359</code> would halt the firewall at one minute to midnight on January 31, 2006.
<code>shutdown -p [time]</code>	Completely powers off the system without restarting. For example, <code>shutdown -p now</code> would immediately shut down the firewall.

Command	Type of shutdown
<pre>shutdown [-rh] -s soft_time time</pre>	<p>A load sharing HA cluster always performs a soft shutdown. A soft shutdown provides a buffer period before the actual shutdown occurs.</p> <p>By default, the soft shutdown process will begin 30 minutes before a scheduled shutdown. If the shutdown is scheduled to occur in less than 30 minutes, the soft shutdown process will begin immediately and will remain in effect until the actual shutdown time occurs.</p> <p>You can schedule a specific shutdown time for a cluster, or a number of minutes until the shutdown, by using <code>-s</code>. For example:</p> <pre>shutdown -r -s +45 +60</pre> <p>(with soft shutdown in 15 minutes, with restart in one hour)</p> <pre>shutdown -r -s 1500 1800</pre> <p>(restart at 6:00, starting soft shutdown at 3:00)</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Note: You must include a soft shutdown time if you use the <code>-s</code> command.</p> </div>

Related concepts

[Scheduling a soft shutdown for a load sharing HA cluster Sidewinder](#) on page 657

Configure the firewall for UPS

Configure the firewall to initiate an orderly shutdown before the UPS fails to avoid an uncontrolled shutdown.

Many organizations connect Sidewinder to an Uninterruptible Power Supply (UPS). This allows the firewall to continue to be operational if a power outage occurs. If the power outage is long enough, however, the battery in the UPS will begin to fail. The firewall is much more likely to restart in a good condition following an orderly shutdown than from an uncontrolled shutdown.

Configure the firewall BIOS for a UPS

Configure BIOS settings before configuring firewall UPS settings.

Steps

- 1) From a console attached to the firewall, log on and enter `srole` to switch to the Admn domain.
- 2) [Conditional] If the UPS device will be connected to the firewall's COM1 port, type the following command:

```
setconsole video
```
- 3) Restart the firewall.

- 4) Enter the firewall BIOS.
- 5) Disable console redirection for the COM port that the UPS will be connected to.
- 6) Save your changes and exit the BIOS.

Configure UPS

Configure the firewall to use a UPS.

Steps

- 1) Connect the UPS's serial cable to the appliance's COM1 or COM2 port. (Use a simple signaling cable.)
 - You must connect the UPS device to the firewall appliance before enabling UPS in the Admin Console. If you enable UPS without an attached UPS device, the firewall might shut down immediately.
 - Each member of an HA cluster must use the same COM port.
- 2) Select **Maintenance > UPS**. The **UPS** window appears.



Tip: For option descriptions, click **Help**.

- 3) Select **Enable Uninterruptible Power Supply (UPS)**.
 - If a UPS is enabled and a power outage occurs, the firewall will monitor the UPS and will perform an orderly shutdown when the UPS battery begins to run low.
 - If a UPS is not enabled, and a power outage occurs, and the appliance *is* connected to a UPS, the firewall will not monitor the UPS and will not perform an orderly shutdown when the UPS battery begins to run low.
- 4) From the **UPS Serial Port** drop-down list, select the port the UPS is connected to.
- 5) In the **Battery Time** field, specify the estimated amount of time (in seconds) that the UPS battery will last before running low. The firewall will initiate an orderly shutdown when this timer expires, regardless of the amount of battery power remaining in the UPS.
- 6) Save your changes.

Register the firewall with Control Center

Use the **Control Center Registration** window to register this Sidewinder to a Control Center Management Server.

- If you chose to auto-register to Control Center during initial configuration of this Sidewinder, do not register with Control Center here. Use the **Sign Up Firewalls** dialog in the Control Center to initiate rapid deployment.
- A Sidewinder administrator account named `ccfwadmin` is automatically created when you register with Control Center. If you already have an administrator account with that name, it will be overwritten.

To register this firewall with Control Center, select **Maintenance > Control Center Registration**. The **Control Center Registration** window appears.

To register this firewall:

Steps

- 1) In the **Name** field, enter the host name of the Management Server that will manage this firewall. If you are also using backup servers, use the host name of the active Management Server.



Tip: For option descriptions, click **Help**.

- 2) In the **IP Address** field, enter the IP address of the Management Server.



Note: Do not use an IPv6 address.

- 3) [Optional] If you are using a High Availability Management Server configuration, select the **Configure backup server** checkbox.
 - a) In the **Backup Server Name** field, enter the host name of the Management Server acting as a backup to the active Management Server.
 - b) In the **IP Address** fields, enter the IP address of the corresponding backup servers.
- 4) Click **Register with the Control Center now**. Click **Yes** to confirm your changes. The **Authentication** window appears.
- 5) Enter the user name and password of the Control Center administrator, then click **OK**. A “registration succeeded” message appears.
- 6) Click **OK**.

Result

To complete registration, go to the Management Server Configuration Tool.

Manage service updates

Use the **Updates** window to update the following services.

- **A/V signatures** — Downloads and installs the latest virus scanning signature files; you can also automatically update the scanner engine
- **Application signatures** — Downloads and installs the latest application signatures
- **Geo-Location database** — Updates the Geo-Location database with the latest country IP information
- **IPS signatures** — Downloads and installs the most current signatures for IPS inspection
- **Messages from Forcepoint** — Downloads the latest messages about software releases, signature and anti-virus engine updates, hardware end-of-life and end-of-support information, patches, and other critical product information
- **SmartFilter updates** — Downloads URL categories from the SmartFilter XL Database

You can schedule automatic updates or update an area manually. To update a service:

Steps

- 1) Select **Maintenance > Updates**. The **Updates** window appears.



Tip: For option descriptions, click **Help**.

- 2) In the list in the upper pane, select a service to update. The configuration settings appear in the lower pane.
- 3) Verify the update source information.
- 4) Perform the action you want.
 - To update the service manually, click **Update Database Now**.
 - To configure automatic updates, select the options in the lower pane, then save your changes.

Editing files

You might need to modify a text file or a configuration file. Although the typical UNIX editors are available (vi and emacs), you might find it easier to use the File Editor provided with the Admin Console.

The File Editor simplifies the editing process, enabling you to perform virtually every necessary editing task from the Admin Console instead of using a command line.

The File Editor also provides some additional conveniences such as unique file backup and restore features. (UNIX aficionados are still welcome to use the editor of their choice if they prefer.) In addition, using the File Editor through the Admin Console provides a secure connection.

In general, use the Admin Console for configuration changes. If you do not have much command line experience, only edit files manually when instructed to do so by the documentation or technical support. If you have experience using the command line, remember that files could have been altered for security reasons and therefore might not behave as you expect. For all administrators, create a backup file before making changes so that you can, if necessary, quickly return your firewall to a functional configuration.

Understanding Sidewinder files

Sidewinder files are not protected against simultaneous editing by two individuals. Whoever saves the file last usually prevails. In some cases, file corruption occurs.



CAUTION: An administrator should take care not to make changes to a file when another administrator is working on it.

For example, if an administrator is editing the `server.conf` configuration file using the Admin Console's File Editor while someone else is using a text editor to change that file, there might be undesirable results. If two people try editing the same file and both are using vi or both are using emacs, however, the editor will warn the users about the situation.

A frequent error to be aware of when manually editing the Sidewinder configuration files (`server.conf`, `roles.conf`, etc.) is the misuse of special characters that are used to format commands within these files. Special characters include double quotes, single quotes, brackets ([]), the pound symbol (#), and parenthesis (). Inadvertently placing special characters in the configuration files will render the files unreadable to the firewall. Enter `man sidewinder.conf` at a command prompt for details.



Note: Save any scripts you create for the firewall in the /usr/local/bin directory. During software upgrades, the upgrade procedure will automatically save any scripts that reside in that directory.

Using the File Editor

The File Editor helps to open and modify files.

To access the File Editor, select **Maintenance > File Editor**, then click **Start File Editor**. The **File Editor** window appears.



Tip: For option descriptions, click **Help**.

The **File Editor** window contains three different menu options:

- **File** — This menu contains the basic action options. Use it to open new or existing files, and to save files. The **File** menu also provides two unique capabilities: it enables you to create a backup copy of a file, and it enables you to restore a file from a previously saved backup copy.
- **Edit** — Use the functions in this menu to cut, copy, paste, and find/replace text.
- **Help** — The following options are available under this menu:
 - **File Editor Help**— Displays specific information for the **File Editor** window.
 - **About Help**— Displays information about the current version of the Admin Console software.

Related tasks

[Create a backup file in the File Editor](#) on page 603

[Restore a file](#) on page 603

[Find/Replace strings](#) on page 604

Open and save files in the File Editor

Open a file or save a file with a different name or location.

From the **File** menu, select **Open** or **Save As**. The **Open File** or **Save As** window appears.

To open or save a file:

Steps

- 1) In the **Source** field, select where the source is located:
 - **Local File** — Indicates the file is located on the local Windows computer or on a network connected to the computer.
 - **Firewall File** — Indicates the file is located on the firewall.



Tip: For option descriptions, click **Help**.

- 2) In the **File** field, type the full path name of the file.
If you do not know the full path name, click **Browse** to browse the available directories. When you locate the file, click **OK**. The file name appears in the **File** field.

- 3) Click **OK** to open or save the file, or click **Cancel** to cancel the request.

Create a backup file in the File Editor

When modifying firewall configuration files, it is normally a good practice to create a backup copy of the file before you begin editing the file. That way, if you make a mistake while editing the file you can revert to the original file.

The File Editor provides an easy method for creating a backup copy of a file. You can even make a backup after you begin modifying a file. The key is to create the backup before you save your changes. Once you save your changes you will not be able to create a backup file that mirrors the original file.

To make a backup copy of a file, open the file. From the **File** menu, select **Backup**. The **Backup File** window appears.

Steps

- 1) In the **Name of Backup File** field, specify a name for the backup file. By default, the file is given the same name as the original file but with a **.bak** extension.

The backup file will be created in the directory listed in the **Current Directory** field. This is the directory in which the original file currently resides, and cannot be modified.



Tip: For option descriptions, click **Help**.

- 2) Click **OK** to save the information and exit the window, or click **Cancel** to exit the window without saving the backup file.

Restore a file

Use the Restore function to restore a file to its original contents.

- The file must be open within the File Editor.
- You must have previously created a backup copy of the file.

From the **File** menu, select **Restore**. The **Restore File** window appears.

Steps

- 1) In the **Restore From File** field, specify the name of the backup file to use when restoring the file to its original condition. If you do not know the name of the backup file, click **Select** to browse the available files. When you locate the file, click **Open**. The file name appears in the **Restore From File** field.



Note: If a backup file exists, it will appear in the same directory as the current file, because you are only allowed to create a backup in the same directory. The **Current Directory** field displays the name of that directory and cannot be modified.



Tip: For option descriptions, click **Help**.

- 2) Click **OK** to save the information and exit the window, or click **Cancel** to exit the window without restoring from the backup file.

Find/Replace strings

Use the **Find/Replace** function to locate character strings, and to replace them with different character strings.

Steps

- 1) From the **Edit** menu, select **Find/Replace**. The **Find/Replace** window appears.



Tip: For option descriptions, click **Help**.

- 2) In the **Find what** field, specify the character string you want to search for within the file.
- 3) [Optional] If you want to replace the character string specified in the **Find what** field with a different character string, type the new string in the **Replace with** field.
- 4) In the **Search** field, specify which direction in the file the search should be performed:
 - **Down** — From your current position within the file, the File Editor will search down (forward) in the file for the specified character string.
 - **Up** — From your current position within the file, the File Editor will search up (backward) in the file for the specified character string.
- 5) In the **Case** field, specify whether the File Editor should find any matching character string, or if it should consider upper and lower case when performing the search:
 - **Match** — Find only those character strings that exactly match the case as specified in the **Find what** field.
 - **Ignore** — Find all matching character strings regardless of upper and lower case.
- 6) Click **Find Next** to start the character search and to locate the next occurrence within the file.
[Optional] If the character search locates a match, you can click **Replace** to replace the found character string with the character string specified in the **Replace with** field. To replace all occurrences of the character string, click **Replace All**. An Info window will appear indicating how many times the character string was replaced. Click **OK** to close the Info window.
- 7) To find additional occurrences of the character string, continue to click **Find Next** for each occurrence. When there are no additional occurrences, a message will appear telling you that the search is complete.
- 8) When you are finished searching, click **Close** to exit this window.

Check file and directory permissions (ls command)

Standard UNIX permits access to files based on a process user and group identifiers and the file's permissions (mode bits that indicate who can read, write, or execute a file).

The Sidewinder Type Enforcement mandatory security policy is the ultimate authority on if, and when, a given process might access files and it overrides standard UNIX permissions. A Sidewinder file that appears to be accessible based on standard UNIX permissions can be denied by the Type Enforcement (TE) policy.

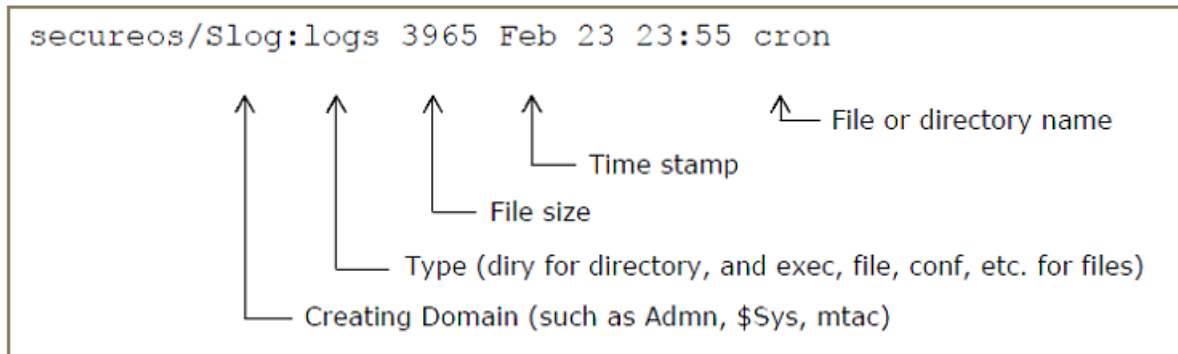
To check Type Enforcement, enter the following commands:

- for files: `/bin/ls -alZ filename`

- for directories: `/bin/ls -dlZ directory_name`

The figure illustrates the output.

Figure 79: Type Enforcement output



Change a file type (chtype command)

Type Enforcement assigns each file and directory a *type*. In general, you should not, and cannot, change this type. In the rare situation where you need to change the type, use the `chtype` command.

To change type on a file or directory:

Steps

- 1) At a command prompt, log on and enter the following command to switch to the Admin role:

```
srole
```

- 2) Copy the file or directory you want to change:

```
cp file1 newfile
```

- 3) Delete the original file:

```
rm file1
```

- 4) Change the new file to the target domain and/or file type:

```
chtype domain:filetype newfile
```

- 5) Rename the file or directory:

```
mv newfile file1
```

Creating scripts

While operating in either the *User* or *Admn* domains, you can create your own scripts for use on the firewall.

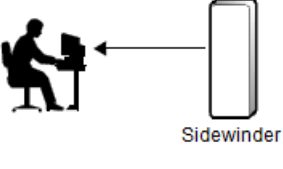
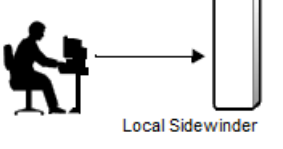
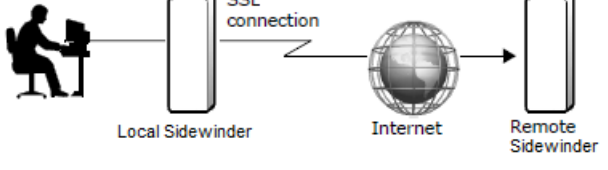
Scripts created in the *User* domain are executable by the *Admn* and *User* domain but no other domain. Scripts created in the *Admn* domain cannot be executed by anyone except the administrator.

Backing up and restoring the firewall configuration

Use the Configuration Backup feature to back up and restore Sidewinder configuration files. Backing up the configuration files lets you quickly restore a firewall to a previous operational state.

The following table shows the three options for a configuration backup.

Table 104: Configuration file backup options

<p>Client system — This option backs up configuration files to the Admin Console computer. This includes any location on your Admin Console hard drive; any removable media with a drive attached to the Admin Console computer, such as diskette or recordable CD; any network drive the Admin Console computer is connected to.</p>	
<p>Local Sidewinder — This option backs up configuration files to the firewall's own hard drive, or to a USB drive. On the firewall, the backup files are stored in the <code>/var/backups/repository</code>; you can move them to another location using a file transfer mechanism such as FTP or SCP.</p>	
<p>Remote system (SCP) — This option backs up configuration files to a remote Sidewinder or to another remote server.</p> <ul style="list-style-type: none"> • SSH access must be enabled on the remote firewall. • A remote server needs SSH enabled (SCP) and a user created. 	

You can also use this feature to manage configuration backups and make a disaster recovery backup.

There are two types of configuration backup files — *Complete* and *Lite*.

- Complete backups are created when backing up configuration files from the **Configuration Backup** tab or from the command line.
- Lite backups are optionally created as part of audit change tickets. Lite backups do not contain home directories or debugging information that technical support uses for troubleshooting.

Access the **Configuration Backup** area by selecting **Maintenance > Configuration Backup**. From this area, you can access the **Configuration Restore** and **Schedule** tabs.

Back up configuration files

Back up Sidewinder configuration files.

- You can back up configuration files to the Admin Console computer, the Sidewinder, or a remote system.

- Only configuration files are backed up with this process. For example, the mail queues, the audit trail, the log files, or executable files will not be backed up in a configuration backup.

Related tasks

[Create a disaster recovery backup](#) on page 610

Back up configuration files to the Admin Console computer

Back up a firewall configuration to the Admin Console computer.

Steps

- 1) In the **Backup Sidewinder Configuration** area, select **Client System**.



Tip: For option descriptions, click **Help**.

- 2) Click **Backup now**. The **Save Configuration Backup** window appears.
- 3) Navigate to the location on the Admin Console computer where you want to save the configuration files. You can select any directory, media drive, or network available to the Admin Console computer.
- 4) [Optional] In the **File name** field, enter a name that can easily identify this configuration backup. A default name consisting of the firewall name plus the current date automatically populates this field.
- 5) Click **Save**. The **Filename and encryption** window appears. Enter the key again to verify.
- 6) For option descriptions, click **Help**. [Optional] Enter a key to encrypt the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ().
 - This key will not be saved. You must remember it. You will not be able to restore the configuration file without this key.
 - You do not have to enter an encryption key. If you click **OK** without entering an encryption key, the backup continues.
- 7) Click **OK**. A "Configuration backup successful" message appears.
- 8) Click **OK**.

Result

You have finished backing up a configuration file to the Admin Console computer.

Back up configuration files to the Sidewinder

Back up a firewall configuration.

Steps

- 1) In the Backup Sidewinder Configuration area, select **Local Forcepoint Sidewinder**.



Tip: For option descriptions, click **Help**.

- 2) Click **Backup now**.
The **Filename and encryption** window appears.
For option descriptions, click **Help**.
- 3) [Optional] In the **File name** field, enter a name that can easily identify this configuration backup.
A default name consisting of the firewall name plus the current date automatically populates this field.
- 4) Select a location for the backup file:
 - To save the backup file on the firewall, select **Disk**.
 - To save the backup file on a USB drive inserted in the USB port on the firewall, select **USB Flash Drive**.
 - Insert the USB drive before performing the backup.
 - Do not remove the USB drive from the firewall until the "Configuration backup successful" message appears
- 5) [Optional] Enter a key to encrypt the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ().
 - This key will not be saved. You must remember it. You will not be able to restore the configuration file without this key.
 - You do not have to enter an encryption key. If you click **OK** without entering an encryption key, the backup continues.

Enter the key again to verify.

- 6) Click **OK**.
A "Configuration backup successful" message appears.
- 7) Click **OK**.
The backup appears in the list of current local configuration backups.

Result

You have finished backing up a configuration file to the firewall.

Back up configuration files to a remote system

Back up a firewall configuration to a remote system.

Before you begin

- If you are backing up to a remote Sidewinder, SSH access must be enabled on the remote firewall.
- If backing up to another remote system, the remote system needs SSH enabled (SCP) and a user created.

Steps

- 1) In the **Backup Sidewinder Configuration** area, select **Remote System (SCP)**.



Tip: For option descriptions, click **Help**.

- 2) Define the remote system that is receiving the configuration backup files:
 - In the **Username** field, enter the user name of a user on the remote system. If the remote system is a Sidewinder, this is a firewall administrator.
 - [Optional] In the **Password** field, enter the password used to authenticate the user to the remote system. The firewall does not save the password. In the **Hostname** field, enter the host name or the IP address of the remote system.
 - The **Port** field default is **22**.
 - In the **Directory** field, enter the directory on the remote system where the configuration files are stored. If the remote system is a Sidewinder, the administrator's home directory is the default.

This information is retained. You can change it at any time.

- 3) Click **Backup now**. The **Filename and encryption** window appears.
For option descriptions, click **Help**.
- 4) [Optional] In the **File name** field, enter a name that can easily identify this configuration backup.
A default name consisting of the firewall name plus the current date automatically populates this field.
- 5) [Optional] Enter a key to encrypt the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ().
 - This key will not be saved. You must remember it. You will not be able to restore the configuration file without this key.
 - You do not have to enter an encryption key. If you click **OK** without entering an encryption key, the backup continues.

Enter the key again to verify.

- 6) Click **OK**. A "Configuration backup successful" message appears.
- 7) Click **OK**.

Result

You have finished backing up a configuration file to a remote system.

Create a disaster recovery backup

Use this feature to create a disaster recovery backup. If you need to re-install your firewall, you can use this backup to restore the configuration.

- The disaster recovery backup saves configuration files, installed packages, and the Quick Start Wizard data file (qsw_datafile) to a USB drive plugged into the appliance.
- The backup can take several minutes to complete.

To create a disaster recovery backup file:

Steps

- 1) Insert a USB drive into the USB port of the Sidewinder appliance.
- 2) On the Admin Console, select **Maintenance > Configuration Backup**.
- 3) Click **Create Disaster Recovery Backup**. The **Configuration Backup Disaster Recovery** window appears.



Tip: For option descriptions, click **Help**.

- 4) [Optional] Enter a key to encrypt the disaster recovery backup. Valid values include alphanumeric characters, periods (.), dashes (-), and underscores (_).
 - This key will not be saved. You must remember it. You will not be able to restore the disaster recovery backup without this key.
 - You do not have to enter an encryption key. If you click **OK** without entering an encryption key, the backup continues.

Enter the key again to verify.

- 5) Click **OK**. A warning message appears.
- 6) Click **Yes** to confirm the backup.
A progress bar appears while the files are backed up to the USB drive.



Note: Do not remove the USB drive from the firewall until the 'Disaster recovery successful' message appears.

When the backup is complete, a 'successful' message appears.

- 7) Click **OK**.
- 8) Remove the USB drive from the appliance and store it in a safe place.
You can restore the disaster recovery backup only during re-imaging.

Related concepts

[Disaster recovery](#) on page 697

Restore a firewall configuration

Use the **Configuration Restore** tab to restore a Sidewinder to a previous operational state. You can also manage local configuration backups.



Tip: For option descriptions, click **Help**.

You can perform the following actions.

- Restore configuration backups
- Manage configuration backup files

Restore configuration backups

Use this feature to restore a Sidewinder to a previous operational state.

- You can restore configuration files from the Admin Console computer, the Sidewinder, or a remote system.
- Only configuration files are restored with this process. For example, the mail queues, the audit trail, the log files, or executable files will not be restored from a configuration backup.
- The backup file must be at the same version as the system it is being restored to.

Restore configuration files from the Admin Console

Restore configuration files from an Admin Console computer.



Note: The firewall will restart after the configuration files have been restored.

Steps

- 1) Select **Client System**.



Tip: For option descriptions, click **Help**.

- 2) Click **Browse** and navigate to the location where the backup file is stored. Select the backup file and click **Open**. The backup file appears in the **Filename** field.
You can also type the path and file name in the **Filename** field.
- 3) Click **Restore now**. A message appears stating that a system restore will cause a restart of the firewall.
- 4) Click **Yes**. The **Filename and encryption** window appears.
- 5) [Optional] Enter an encryption key to restore the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ().
Enter the key again to verify.



Note: If you did not enter an encryption key during the configuration backup, click **OK** to continue with the restore.

- 6) Click **OK**. When the restore is complete, a “Configuration restore successful” message appears.

- 7) Click **OK**. Your Admin Console is disconnected while the firewall restarts.

Result

You have finished restoring a configuration backup from the Admin Console.

Restore configuration files from the firewall

Restore configuration files from Sidewinder.



Note: The firewall will restart after the configuration files have been restored.

Steps

- 1) Select **Local Forcepoint Sidewinder**.



Tip: For option descriptions, click **Help**.

- 2) From the list of configuration backups, select the configuration you want to restore to the firewall. If the configuration backup is on a USB drive, insert the USB drive in the firewall's USB port, then click the **Refresh** button to see the configuration backup in the list.
- 3) Click **Restore now**. A message appears stating that a system restore will cause a restart of the firewall.
- 4) Click **Yes**. The **Filename and encryption** window appears.
- 5) [Optional] Enter an encryption key to restore the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces (). Enter the key again to verify.



Note: If you did not enter an encryption key during the configuration backup, click **OK** to continue with the restore.

- 6) Click **OK**. When the restore is complete, a "Configuration restore successful" message appears.
- 7) Click **OK**. Your Admin Console is disconnected while the firewall restarts.

Result

You have finished restoring a configuration backup from the Sidewinder.

Restore configuration files from a remote system

You can restore configuration files from a remote system.



Note: The firewall will restart after the configuration files have been restored.

Steps

- 1) Select **Remote System (SCP)**.



Tip: For option descriptions, click **Help**.

- 2) In the **Filename** field, enter the name of the configuration backup file you are restoring.
- 3) Define the remote system where the configuration backup files are stored.
 - In the **Username** field, enter the user name of a user on the remote system. If the remote system is a Sidewinder, this is a firewall administrator.
 - [Optional] In the **Password** field, enter the password used to authenticate the user to the remote system.



Note: The firewall does not save the password.

- In the **Hostname** field, enter the host name or the IP address of the remote system.
- The **Port** field default is **22**.
- In the **Directory** field, enter the directory on the remote system where the configuration files are stored. If the remote system is a Sidewinder, the administrator's home directory is the default.

This information is retained. You can change it at any time.

- 4) Click **Restore now**. A message appears stating that a system restore will cause a restart of the firewall.
- 5) Click **Yes**. The **Filename and encryption** window appears.
- 6) [Optional] Enter the key you used to encrypt the configuration backup file. Valid values include alphanumeric characters, periods (.), dashes(-), underscores (_), and spaces ().
Enter the key again to verify.



Note: If you did not enter an encryption key during the configuration backup, click **OK** to continue with the restore.

- 7) Click **OK**. A warning message appears asking if you want to disconnect after starting the restore.
- 8) Click **Yes**. When the restore is complete, a "Configuration restore successful" message appears.
- 9) Click **OK**. Your Admin Console is disconnected while the firewall restarts.

Result

You have finished restoring a configuration backup from a remote system.

Manage configuration backups

Use the **Current local configuration backups** list to view, move, and compare configuration backup files.

You can access the **Current local configuration backups** list from two tabs:

- **Configuration Backup** tab — Select **Maintenance > Configuration Backup**.


- **Configuration Restore tab** — Select **Maintenance > Configuration Backup > Configuration Restore**, then select **Local Forcepoint Sidewinder**.



Note: Any changes to the list on the **Configuration Restore** tab also appear on the **Configuration Backup** tab.



Tip: For option descriptions, click **Help**.

Task	Steps
Delete a configuration backup from the firewall file system	<ol style="list-style-type: none"> 1) Select a configuration backup from the list. 2) Click Delete. Click Yes to confirm the deletion.
Move a configuration backup from the Admin Console computer to the firewall	<ol style="list-style-type: none"> 1) Click Upload. The Upload Configuration Backup window appears. 2) Navigate to the location on the Admin Console computer where the configuration backup file is stored. 3) Select the configuration backup file and click Open. An “Upload successful” message appears when the upload is complete. 4) Click OK. The backup file appears in the list.
Move a configuration backup from the firewall to the Admin Console computer	<ol style="list-style-type: none"> 1) Select a configuration backup file from the list. 2) Click Download. The Save Configuration Backup window appears. 3) Navigate to the location on the Admin Console computer you want to copy the backup file to. <div data-bbox="704 1304 1459 1457" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Tip: This can include a directory on the hard drive, removable media with a drive attached to the Admin Console computer, or a network drive the Admin Console computer is connected to.</p> </div> 4) Click Save. A “Download successful” message appears when the download is complete. 5) Click OK.

Task	Steps
Compare the policy of configuration backups	<ol style="list-style-type: none"> 1) Select configuration backups to compare: <ul style="list-style-type: none"> • To compare the changes between a configuration backup and the current running configuration, select the backup file from the list. • To compare the changes between two configuration backups, select the two backup files from the list. 2) Click Compare. The Compare Backups window appears. 3) Review the changes. 4) Click Close.
View audit data for a configuration backup	<ol style="list-style-type: none"> 1) Select a Lite configuration backup file from the list. 2) Click Audit. The View Audit Data window appears. 3) When you are done viewing the data, click Close.

Schedule configuration backups

You can back up configuration files to the Sidewinder, a USB drive, or a remote system.

Use **Schedule** tab to schedule automatic configuration backups.

Steps

- 1) Select **Enable scheduled configuration backups**. If this checkbox is cleared, scheduled configuration backups will not occur.



Tip: For option descriptions, click **Help**.

- 2) Select the backup destination.
 - If you select **Local Forcepoint Sidewinder**:
 - To save the backup file on the firewall, select **Disk**.
 - To save the backup file on a USB drive inserted in the USB port on the firewall, select **USB Flash Drive**.
 - Select whether you want to keep all backups or configure a number of backups to keep.
 - If you select **Remote System (SCP)**, define the remote system that is receiving the configuration backup files:
 - In the **Username** field, enter the user name of a user on the remote system. If the remote system is a Sidewinder, this is a firewall administrator.
 - In the **Password** field, enter the password used to authenticate the user to the remote system. (The firewall does not save the password.)
 - In the **Hostname** field, enter the host name or IP address of the remote system.
 - The **Port** field default is **22**.

- In the **Directory** field, enter the directory on the remote system where the configuration files are stored. If the remote system is a Sidewinder, the administrator's home directory is the default.

This information is retained. You can change it at any time.

3) Configure the backup schedule:

- **Frequency** — From the drop-down list, select the frequency for exporting the file (hourly, daily, or weekly).
 - If you selected **Hourly**, enter the number of minutes after the hour.
 - If you selected **Daily**, enter the time for export.
 - If you selected **Weekly**, enter the time and day. You can select multiple days.
 - [Conditional] To define a custom frequency for exporting files, select **Custom** and complete the fields. Refer to `man 5 crontab` for options.
- **Command** — Displays the backup that will be executed.
- **Description** — A default description populates this field. If desired, enter a descriptive name for the task.

Make the firewall FIPS 140-2 compliant

For instructions on how to make the firewall compliant with Federal Information Processing Standard (FIPS) 140-2, refer to the *Firewall Enterprise FIPS 140-2 Configuration Guide*.

Certificate/key management

Contents

- [Managing certificates](#) on page 617
- [Managing remote identities](#) on page 633
- [Managing keys](#) on page 634

Certificates are used for host validation in many connections. Keys are used on the firewall for encrypted SSH and SSL connections.

Managing certificates

You can use certificates for content inspection, authentication, and identity management.

Why use certificates

Certificates are used to verify the identity and authenticity of hosts during electronic communication.

A certificate can be thought of as the digital equivalent of a driver's license. Certificates associate a user or device with a public/private key pair for use with public key cryptography.

Public key cryptography, also known as asymmetric cryptography, is an encryption method in which each participant has a private key that is kept secret and a public key that can be distributed to anyone. The public and private keys are mathematically related so that data that is encrypted using one key can only be decrypted using the corresponding key. Certificates and public key cryptography are used in the Secure Sockets Layer (SSL) protocol.

Sidewinder uses certificates for:

- SSL content inspection
- VPN authentication and identity management
- Communication with other products
- Firewall administrative services, such as the Admin Console and Sidewinder Control Center
- Miscellaneous firewall services

Certificate trust

A certificate's distinguished name (DN) identifies who it belongs to, but without third-party verification it cannot be trusted that the DN matches the real identity of the certificate holder. In the public key cryptography system, the third-party verifier is called a certificate authority (CA).

To prove that a certificate is trustworthy, it must be signed by a mutually trusted CA. You can get a certificate signed.

- 1) The owner of the certificate submits the certificate to a CA.
- 2) The CA attempts to verify:
 - The owner's identity in the real world
 - That the owner controls the private key associated with the public key in the certificate
- 3) If the CA successfully verifies the certificate holder's identity and private key, it signs the certificate.

Because the certificate has been signed by a CA, other parties know it can be trusted.

Understanding Distinguished Name syntax

A DN is a unique, unambiguous name that identifies the holder of a certificate. This section summarizes the DN string syntax through a series of examples.

As defined in the X.500 specifications, a DN is an Abstract Syntax Notation One (ASN.1) value. In an X.509 certificate, a DN is represented as a binary value, but Sidewinder uses the string syntax defined by RFC 2253 to display the DN in a human-readable format.



Note: For more information on this string syntax, see RFC 4514 at <http://www.ietf.org/rfc.html>.

A DN consists of a sequence of *identity components*, each composed of a type tag and a value. The components of a DN are sets of attribute type/value pairs. The *attribute type* indicates the type of the item, and the *attribute value* holds its contents. Each type/value pair consists of an X.500 attribute type and attribute value, separated by an equal sign (=). In the example CN=Jane Smith, “CN” is the attribute type and “Jane Smith” is the value.

The attribute type/value pairs are separated by commas (.). This example shows a DN made up of three components:CN=Jane Smith,OU=Sales,O=Forcepoint

Plan out your organization's certificate identification needs before creating any DNs. DNs have a hierarchical structure, reading from most specific to least specific. No preset hierarchy of attribute type exists, but the structure for a given organization needs to be consistent. In this example, the organization Forcepoint has organizational units, making the organizational unit attribute type more specific than the organization attribute type.

CN=Jane Smith,OU=Sales,O=Forcepoint

CN=Ira Stewart,OU=Engineering,O=Forcepoint

An attribute type is specified by a tag string associated with the X.500 attribute being represented. Sidewinder supports the attribute tag strings displayed in the table below, which includes the most common ones recommended by RFC 2253. The tag strings are not case sensitive.

Table 105: Supported X.500 attribute type tags

Tag String	X.500 Attribute Name	Character String Type	Maximum Number of Characters
C	CountryName	PrintableString	2
CN	CommonName	DirectoryString	64
EmailAddress	EmailAddress	IA5String	128
L	LocalityName	DirectoryString	128
O	OrganizationName	DirectoryString	64

Tag String	X.500 Attribute Name	Character String Type	Maximum Number of Characters
OU	OrganizationUnitName	DirectoryString	64
SN	Surname	DirectoryString	128
ST	StateName	DirectoryString	128
Street	StreetAddress	DirectoryString	128
UID	UserID	DirectoryString	128

The attribute value contains the content of the identity information, and is constrained by the associated attribute type. For the supported attribute types, the preceding table shows the corresponding string type (which limits the allowed set of characters) and its maximum length. For example, given “CN=Jane Smith” as a name component, the string “Jane Smith” is of type DirectoryString, and is constrained to a maximum of 64 characters. The maximum number of characters allowed in a DN (that is, the number of characters for all attribute values added together) is 1024.

The following table defines the allowed character set for each character string type.

Table 106: Character string types

Character String Type	Allowed Characters
PrintableString	A–Z, a–z, 0–9, ()+-./:=?, comma (,), space (' '), apostrophe (”)
DirectoryString	All 8 bit characters without encoding, All non–8 bit characters with UTF–8 encoding
IA5String	All ASCII characters

The following characters have special meaning in the string syntax and must be preceded by a backslash character (\):

- comma (,)
- equal sign (=)
- plus sign (+)
- less than sign (<)
- greater than sign (>)
- pound sign (#)
- semicolon (;)
- backslash (\)
- quotation (“ ”)

All other printable ASCII characters represent themselves. Non-printable ASCII must be have a backslash preceding the ordinal value of the character in two-digit hexadecimal (for example, the BEL character, which has an ordinal value of seven, would be represented by \07). Here are some examples of the escape conventions:

```
CN=Jane Smith\,DDS,OU=Sales,O=Forcepoint
```

```
CN=\4a\61\6e\65\20Smith,OU=Sales,O=Forcepoint
```

Attribute values might optionally be contained within double-quote characters, in which case only the backslash (\), double quote (“ ”), and non-printable ASCII characters need to be preceded by a backslash. Here the double-quotes eliminate the need to escape the CN’s comma:

```
CN="Jane Smith,DDS",OU=Sales,O=Forcepoint
```



Note: Entries containing backslashes or double-quotes will appear “normalized” (without extra characters or spaces) in the user interface once they are saved.

Use string syntax when entering DN's using the Admin Console.



Note: For additional information on DN syntax, see RFCs 2044, 2252, 2253, and 2256.

Managing firewall certificates

A firewall certificate identifies the firewall to a potential peer in certain scenarios.

- VPN authentication
- Inbound SSL content inspection
- Firewall administration services

When creating a certificate for the firewall, you have the option to submit the certificate to a CA to be signed or have the firewall generate a self-signed certificate.


Select **Maintenance > Certificate/Key Management**, then select the **Firewall Certificates** tab. The **Firewall Certificates** tab appears.



Tip: For option descriptions, click **Help**.

Table 107: Firewall certificate management tasks

Task	Steps
View the properties of a firewall certificate	<p>Select the certificate from the list. Its properties are displayed on the right portion of the window.</p> <p> Tip: You can view additional properties by exporting the certificate to screen.</p>
Create a firewall certificate	<p>Click New. The Create New Certificate window appears.</p>
Delete a firewall certificate	<p>Select the appropriate certificate, then click Delete.</p> <p> Note: A certificate cannot be deleted if it is currently in use.</p>
Import a firewall certificate	<p>Click Import. The Import Certificate window appears.</p>
Export a firewall certificate	<p>Select the appropriate firewall certificate, then click Export.</p> <p> Tip: The export function is generally used when capturing the certificate information needed by a remote partner such as a VPN client.</p>

Task	Steps
Retrieve a certificate	<p>To load a signed certificate request from a CA:</p> <ul style="list-style-type: none"> If a certificate request has been submitted to be signed by a CA, click the Query button to query the CA to see if the certificate is approved. If yes, the Status field will change to <i>SIGNED</i> and the approved certificate will be retrieved. If the certificate request is Manual PKCS10, click the Load button to load the signed certificate from a file supplied by the CA. <p> Note: By default, Netscape CAs and CAs that support the Simple Certificate Enrollment Protocol (SCEP) are checked every 15 minutes for any signed certificates waiting to be retrieved.</p>

Related tasks

[Export certificates](#) on page 627

[Create firewall certificates](#) on page 621

[Import firewall certificates](#) on page 622


[Load manually signed certificates](#) on page 627

Create firewall certificates

Create a certificate for the firewall to use to identify itself in a connection.

Steps

- 1) Select **Maintenance > Certificate/Key Management**.
- 2) Select the **Firewall Certificates** tab. The **Firewall Certificates** tab appears.

 **Tip:** For option descriptions, click **Help**.
- 3) Click **New**. The **Create New Certificate** window appears.
- 4) In the **Certificate Name** field, type a name for this certificate.
- 5) In the **Distinguished Name** field, create a distinguished name.
- 6) [Optional] Create one or more alternate identities for the certificate.
 - a) In the **Alternate identities** area, click **New**. A row appears in the list of identities.
 - b) In the **Identity** column, select the appropriate identity type.
 - c) In the **Value** column, type the identity value.



Note: Some CAs do not support alternate identities.

- 7) In the **Key type** area, select the public key type associated with the certificate.
- 8) From the **Key length** drop-down list, select a length in bits for the certificate's public/private key pair.
- 9) From the **Digest** drop-down list, select a secure hash algorithm associated with the certificate.
- 10) From the **Submit to CA** drop-down list, select the enrollment method to which the certificate will be submitted for signing.
 - **Self Signed** — Indicates the new certificate will be signed by the firewall rather than by a CA.
 - **Manual PKCS10** — Indicates the certificate enrollment request will be placed in a PKCS10 envelope and exported to the file designated in the **Generated PKCS10 File** field.
 - The name of the Netscape 4.2 or SCEP CA to submit the certificate to. The CA must first be defined on the **Certificate Authorities** tab.
- 11) [Conditional] Depending on the method you selected in the **Submit to CA** field, the **Other Parameters** area might contain additional fields, as described below:
 - If you selected **Manual PKCS10**, complete the following fields:
 - **Generated PKCS10 File** — Specify the name and location of the file that contains the signed certificate, or click **Browse** to locate the file.
 - **Format** — Select the appropriate format for your PKCS10 certificate request.
 - If you selected a method that uses SCEP, type a password in the **SCEP Password** field.
- 12) Click **Add** to add the certificate to the **Certificates** list.
- 13) Save your changes.

Related concepts

[Understanding Distinguished Name syntax](#) on page 618

Import firewall certificates

Import a certificate for the firewall to use to identify itself in a connection.



Note: The displayed fields vary depending on which import source you select.

Steps

- 1) Select **Maintenance > Certificate/Key Management**.
- 2) Select the **Firewall Certificates** tab. The **Firewall Certificates** tab appears.



Tip: For option descriptions, click **Help**.

- 3) Click **Import**. The **Import Certificate** window appears.

- 4) In the **Import source** field, select **File** or **Encrypted File (PKCS12)**.



Note: The available fields vary based on the import source you select.

- 5) In the **Certificate Name** field, type a local name for the certificate you are importing.
- 6) Specify the location of the certificate file(s) you are importing based on the import source you selected.
 - **File** — Complete the following fields:
 - **Import Certificate From File** — Type the path and name of the certificate file, or click **Browse** to navigate to the file.
 - **Import Private Key from file** — Type the path and name of the private key file, or click **Browse** to navigate to the file. The file can be in either PK1 or PK8 format.
 - **Encrypted File (PKCS12)** — Complete the following fields:
 - **Import Certificate/Key From File** — Type the path and name of the certificate file, or click **Browse** to navigate to the file.
 - **Password** — Enter the password required to decrypt the imported file.
- 7) Click **OK**, then save your changes.

Assigning certificates for firewall services

Firewall services typically use the default SSL certificate, which is uniquely generated during firewall installation. If necessary, you can assign different firewall certificates to firewall services.



Tip: You can create replacement certificates on the **Firewall Certificates** tab. See *Create firewall certificates*.

To assign a new certificate to a firewall service, select **Maintenance > Certificate/Key Management**, then click the **SSL Certificates** tab. The **SSL Certificates** tab appears.

Each firewall service is protected by a custom proxy. To assign a new certificate to a selected proxy, click **Modify**, then select a new certificate to assign to the proxy.



Note: If you click **Modify** and there is not at least one self-signed RSA/DSA firewall certificate currently defined on the firewall, a warning message appears. See *Create firewall certificates* for information on defining this type of certificate.

Related tasks

[Create firewall certificates](#) on page 621

Managing remote certificates

Remote certificates identify peers involved in a VPN connection with the firewall and administrators using Common Access Card authentication.





You can import existing certificates or create new remote certificates.

Select **Maintenance > Certificate/Key Management**, then select the **Remote Certificates** tab. The **Remote Certificates** tab appears.



Tip: For option descriptions, click **Help**.

Table 108: Remote certificate management tasks

Task	Steps
View the properties of a remote certificate	<p>Select the certificate from the list. Its properties are displayed on the right portion of the window.</p> <p> Tip: You can view additional properties by exporting the certificate to screen.</p>
Create a remote certificate	<p>Click New. The Create New Certificate window appears.</p>
Delete a remote certificate	<p>Select the appropriate certificate, then click Delete.</p> <p> Note: A certificate cannot be deleted if it is currently in use.</p>
Import a remote certificate	<p>Click Import. The Import Certificate window appears.</p>
Export a remote certificate	<p>Select the appropriate certificate, then click Export.</p> <p> Tip: Export certificates when they are needed by a remote partner such as a VPN client or when you want to view certificate data.</p>
Retrieve a certificate	<p>To load a signed certificate request from a CA:</p> <ul style="list-style-type: none"> • If a certificate request has been submitted to be signed by a CA, click the Query button to query the CA to see if the certificate is approved. If yes, the Status field will change to <i>SIGNED</i> and the approved certificate will be retrieved. • If the certificate request is Manual PKCS10, click the Load button to load the signed certificate from a file supplied by the CA. <p> Note: By default, Netscape CAs and CAs that support the Simple Certificate Enrollment Protocol (SCEP) are checked every 15 minutes for any signed certificates waiting to be retrieved.</p>

Related tasks

[Export certificates](#) on page 627

[Load manually signed certificates](#) on page 627

[Create a new remote certificate](#) on page 625

[Import a remote certificate](#) on page 626

Create a new remote certificate

Create a certificate for the firewall to use to identify a peer in a connection.

Steps

- 1) Select **Maintenance > Certificate/Key Management**.
- 2) Select the **Remote Certificates** tab. The **Remote Certificates** tab appears.



Tip: For option descriptions, click **Help**.

- 3) Click **New**. The **Create New Certificate** window appears.
- 4) In the **Certificate Name** field, type a name for this certificate.
- 5) In the **Distinguished Name** field, create a distinguished name.
- 6) [Optional] Create one or more alternate identities for the certificate.
 - a) In the **Alternate identities** area, click **New**. A row appears in the list of identities.
 - b) In the **Identity** column, select the appropriate identity type.
 - c) In the **Value** column, type the identity value.



Note: Some CAs do not support alternate identities.

- 7) In the **Key type** area, select the public key type associated with the certificate.
- 8) From the **Key length** drop-down list, select a length in bits for the certificate's public/private key pair.
- 9) From the **Digest** drop-down list, select a secure hash algorithm associated with the certificate.
- 10) From the **Submit to CA** drop-down list, select the enrollment method to which the certificate will be submitted for signing. The valid options are:
 - **Self Signed** — Indicates the new certificate will be signed by the firewall rather than by a CA.
 - **Manual PKCS10** — Indicates the certificate enrollment request will be placed in a PKCS10 envelope and exported to the file designated in the **Generated PKCS10 File** field.
 - The name of the Netscape 4.2 or SCEP CA to submit the certificate to. The CA must first be defined on the **Certificate Authorities** tab.
- 11) [Conditional] Depending on the method you selected in the **Submit to CA** field, the **Other Parameters** area might contain additional fields, as described below:
 - If you selected **Manual PKCS10**, complete the following fields:
 - **Generated PKCS10 File** — Specify the name and location of the file that contains the signed certificate, or click **Browse** to browse for the file.
 - **Format** — Select the appropriate format for your PKCS10 certificate request
 - If you selected a CA that uses SCEP, type a password in the **SCEP Password** field.

- 12) Click **Add** to add the certificate to the Certificates list.
- 13) Save your changes.

Related concepts

[Understanding Distinguished Name syntax](#) on page 618

Import a remote certificate

Import a certificate for the firewall to use to identify a peer in a connection.

Steps

- 1) Select **Maintenance > Certificate/Key Management**.
- 2) Select the **Remote Certificates** tab. The **Remote Certificates** tab appears.



Tip: For option descriptions, click **Help**.

- 3) Click **Import**. The **Import Certificate** window appears.
- 4) In the **Import source** field, select the source location of the certificate.
 - **File** — Indicates you will manually specify the location of the certificate file.
 - **Encrypted File (PKCS12)** — Indicates you will manually specify the location of the file that contains both the certificate and private key.
 - **Paste PEM Certificate** — Indicates you will import the certificate by performing a cut and paste.
- 5) In the **Certificate Name** field, type a local name for the certificate you are importing.
- 6) Specify the location of the certificate you are importing based on the import source you selected.
 - **File** — Type the path and name of the certificate file in the **Import Certificate From File** field, or click **Browse** to navigate to the file's location.
 - **Encrypted File (PKCS12)** — Complete the following fields:
 - **Import Certificate/Key From File** — Type the path and name of the certificate file, or click **Browse** to navigate to the file.
 - **Password** — Enter the password required to decrypt the imported file.
 - **Paste PEM Certificate** — Paste the certificate in the **Pasted PEM Certificate** field.
- 7) Click **OK** to import the remote certificate.
- 8) Save your changes.

Load manually signed certificates

If you created a manually signed firewall or remote certificate, you must retrieve the certificate after it is signed by the CA.

To load a manually signed certificate:

Steps

- 1) Select **Maintenance > Certificate/Key Management**.
- 2) Based on the type of certificate you are loading, click the **Firewall Certificates** tab or the **Remote Certificates** tab.



Tip: For option descriptions, click **Help**.

- 3) Select the appropriate certificate, then click **Load**. The **Load Certificate for PKCS10 Request** window appears.
- 4) Specify the certificate, then click **OK** to load the specified certificate. If available, the certificate is imported and the status changes to **SIGNED**.
- 5) Save your changes.

Export certificates

Export a firewall or a remote certificate.

You can export a certificate to:

- Import it on another device:
 - Remote Certificate — You are most likely to export a remote certificate if you have certificate-based VPN definitions. The VPN client requires the use of a certificate to identify itself during the VPN connection negotiations. You can create a self-signed certificate for the VPN client on the firewall, export it, then import it into the VPN client program.
 - Firewall Certificate — You might export the firewall certificate to install it on a remote peer. This allows the remote peer to recognize the firewall. On the remote peer, the firewall certificate is imported as a remote certificate.
- Back it up independently (certificates are included in configuration backups)
- View its contents in detail



Note: You can also export CA certificates.

Related concepts

[Managing certificate authorities](#) on page 629

Export only the certificate

Export a certificate without the private key.

Steps

- 1) Select **Maintenance > Certificate/Key Management**.
- 2) Choose one of the following, depending on the type of certificate to export:
 - For remote certificates, select the **Remote Certificates** tab. The **Remote Certificates** appears.
 - For firewall certificates, select the **Firewall Certificates** tab. The **Firewall Certificates** appears.



Tip: For option descriptions, click **Help**.

- 3) Select the appropriate certificate, then click **Export**. The **Certificate Export** window appears.
- 4) Select the **Export Certificate (Typical)** radio button.
- 5) Select the export destination:
 - **Export Certificate To File** — To export the certificate to a file, select this option and proceed to Step 3.
 - **Export Certificate To Screen** — Select this option to export the certificate to the screen.
- 6) [Conditional] If you are exporting the certificate to file, do the following:
 - a) In the **File** field, type the name and location of the file to which the certificate will be written, or click **Browse** and navigate to a location to save the certificate file.
 - b) In the **Format** field, select the appropriate format for the file.
- 7) Click **OK** to export the certificate to the desired location.

Export both the certificate and private key

Export a certificate and private key to back it up or to install a self-signed remote certificate on another device.



Note: It is important to protect the private key since it can be used to establish the identity of the certificate holder to peers. If the private key is compromised, another party can impersonate the certificate holder.

Steps

- 1) Select **Maintenance > Certificate/Key Management**.
- 2) Choose one of the following, depending on the type of certificate to export:
 - For remote certificates, select the **Remote Certificates** tab. The **Remote Certificates** appears.
 - For firewall certificates, select the **Firewall Certificates** tab. The **Firewall Certificates** appears.



Tip: For option descriptions, click **Help**.

- 3) Select the appropriate certificate, then click **Export**. The **Certificate Export** window appears.
- 4) Specify whether the certificate and private key will be exported as one file or two files by selecting one of the following options:
 - **Export Certificate and Private Key as one file (PKCS12)** — Select this option to export both the certificate and private key as a single file. We recommend using this format because it encrypts the private key.
 - **Export Certificate and Private Key as two files (PKCS1, PKCS8, X.509)** — Select this option to export the certificate and private key as two separate files.



CAUTION: The private key is not encrypted using this method.

- 5) Specify where to save the exported certificate file(s) based on the export format you selected.
 - **Export Certificate and Private Key as one file (PKCS12)** — Complete the following fields:
 - **File** — Type the name and location of the file to write the certificate to, or click **Browse** and navigate to the location.
 - **Password and Confirm Password** — Type the password you want to use to encrypt the file.
 - **Export Certificate and Private Key as two files (PKCS1, PKCS8, X.509)** — Complete the following fields:
 - **Certificate File** — Type the name and location of the file to write the certificate to, or click **Browse** and navigate to the location. From the **Format** drop-down list, select the appropriate file format.
 - **Private Key File** — Type the name and location of the file to write the private key to, or click **Browse** and navigate to the location. From the **Format** drop-down list, select the appropriate file format.



CAUTION: The private key is not protected when exported individually. If you use a transportable medium to store the private key file, the medium should be destroyed or reformatted after the private key information has been imported on the appropriate device.

- 6) Click **OK** to export the certificate.

Managing certificate authorities

Certificate authorities (CAs) are used to validate certificates for firewall services and sign firewall and remote certificates.

The following table contains the CA types supported by Sidewinder.

Table 109: Supported CA types

CA type	CA location	Purpose
Manual	Remote	Used for conventional certificate validation. <ul style="list-style-type: none"> • To add the CA certificate, the administrator obtains and loads the necessary files. • Subordinate certificates signed by the CA are generated and signed independently of the firewall, and can be manually imported.

CA type	CA location	Purpose
Netscape 4.2	Remote	Used for conventional certificate validation. <ul style="list-style-type: none"> The certificate for the CA is retrieved automatically using a Netscape 4.2 HTTP URL. Certificates can be enrolled to the CA (signed) automatically if allowed by the CA.
SCEP	Remote	Used for conventional certificate validation. <ul style="list-style-type: none"> The certificate for the CA is retrieved using the Simple Certificate Enrollment Protocol (SCEP). The CA can be of any type, such as Entrust or VeriSign, as long as it supports SCEP. Certificates can be enrolled to the CA (signed) automatically if allowed by the CA.
Local	Firewall-hosted	Used to sign server certificates presented to clients when SSL content inspection is enabled.

You can create CA groups in order to reference multiple CAs in SSL or VPN policy.


To manage certificate authorities, select **Maintenance > Certificate/Key Management**, then click the **Certificate Authorities** tab. The **Certificate Authorities** tab appears.



Tip: For option descriptions, click **Help**.

Table 110: Certificate authority management tasks

Task	Steps
Add a CA	<ol style="list-style-type: none"> 1) Click New, then select Single CA. The New Certificate Authority window appears. 2) In the New Certificate Authority window, complete the fields as appropriate. 3) Click Add, then save your changes.
Modify a CA	<ol style="list-style-type: none"> 1) In the Cert Authorities list, select the CA that you want to modify. The properties of the CA appear to the right. 2) Update the CA fields as appropriate. 3) Save your changes.
Create a CA group	<ol style="list-style-type: none"> 1) Click New, then select CA group. The New Certificate Authority Group window appears. 2) In the New Certificate Authority Group window, select CA group members. 3) Click Add, then save your changes.

Task	Steps
Modify a CA group	<ol style="list-style-type: none"> 1) In the Cert Authorities list, select the CA group that you want to modify. 2) Click Modify. The Modify Certificate Authority Group window appears. 3) In the Modify Certificate Authority Group window, select or deselect CA group members. 4) Click OK, then save your changes.
Delete a CA or CA group	<ol style="list-style-type: none"> 1) In the Cert Authorities list, select the CA or CA group that you want to delete. 2) Click Delete. A confirmation pop-up window appears. 3) Click Yes. The CA or CA group is deleted.
Retrieve a CA certificate	<ol style="list-style-type: none"> 1) In the Cert Authorities list, select the CA that you want to retrieve a certificate for. <div data-bbox="581 884 634 940" style="float: left; margin-right: 10px;">  </div> <div data-bbox="667 884 1453 974" style="background-color: #f0f0f0; padding: 5px;"> <p>Note: This option is only available for Netscape4.2 and SCEP CAs.</p> </div> 2) Click Get CA Cert. The firewall attempts to download the CA certificate, and a pop-up window appears. 3) Click OK. The certificate is displayed in in the Distinguished Name (DN) field.
Export a CA certificate	<ol style="list-style-type: none"> 1) In the Cert Authorities list, select the CA that you want to export a certificate for. 2) Click Export. The Certificate Export window appears. 3) In the Certificate Export window, complete the fields as appropriate. 4) Click OK. The CA certificate is exported.
Retrieve a CRL for a CA	<ol style="list-style-type: none"> 1) In the Cert Authorities list, select the CA that you want to download a certificate revocation list (CRL) from. 2) Click Get CRL. The firewall attempts to download the CRL from the CA, and a pop-up window appears. 3) Click OK.

Configure the certificate server

The certificate server performs certificate validation, and retrieves CRLs from CAs.



Note: The certificate server only validates certificates that are signed by CAs defined on the **Certificate Authorities** tab.

To configure the certificate server:

Steps

- 1) Select **Maintenance > Certificate/Key Management**, then click the **Certificate Server** tab. The **Certificate Server** tab appears.



Tip: For option descriptions, click **Help**.

- 2) From the **Audit Level** drop-down list, select the type of auditing to perform for this server.
 - **Error** — Logs only major errors
 - **Normal** — (Default) Outputs major errors and informational messages
 - **Verbose** — Used when initially troubleshooting VPN connectivity problems; this audit output is useful for detecting configuration issues
 - **Debug** — Logs all errors and informational messages; also logs debug information



Note: Only use **Debug** and **Error** if you are an experienced administrator or [Forcepoint support](#) advises you to. In particular, debug can overflow your audit logs if left on for an extended period of time.

- 3) In the **Validated key cache size** field, specify the maximum number of validated keys to store in cache memory.
 - Caching validated keys can increase system performance.
 - Valid values are 0–500.
 - A value of **0** indicates that no keys will be cached.
 - For most systems, a value of **100** is sufficient.
- 4) In the **Validated key cache lifetime** field, specify the maximum amount of time a certificate can remain in the validated key cache before it must be re-validated.
 - The valid range is 0–168 hours (1 week).
 - A value of **0** indicates that the certificate keys must be re-validated with each use.
- 5) From the **CRL retrieval interval** drop-down list, specify how often the certificate server queries CAs for updated CRLs.
- 6) Save your changes.

Managing remote identities

Remote identities identify the authorized users who take part in a VPN definition and have been issued one of the following options.

- Certificate from a particular CA
- VPN client configured with a pre-shared password

Remote identities allow the firewall to perform:

- **Policy selection** — Identity matching identifies which VPN definition should be used for a given VPN peer.
- **Access control** — [Certificate authority-based VPNs] Remote identities narrow the selection of certificates accepted by the firewall.



Note: Remote identities are not used in VPNs that are configured for the Single Certificate authentication method.

To manage remote identities, select **Maintenance > Certificate/Key Management**, then select the **Remote Identities** tab. The **Remote Identities** tab appears.



Tip: For option descriptions, click **Help**.

Table 111: Remote identities management tasks

Task	Steps
Create a remote identity	<ol style="list-style-type: none"> 1) Click New. The Create New Remote Identity window appears. 2) In the Create New Remote Identity window, complete the fields as appropriate. <ul style="list-style-type: none"> • If the remote identity will be used in a Certificate Authority-based VPN definition, configure the Identity Name and Distinguished Name fields. • If the remote identity will be used in a password-based VPN definition, configure the Identity Name field and one or more of the following fields as appropriate: E-Mail Address, Domain Name, or IP Address. 3) Click Add, then save your changes.
Modify a remote identity	<ol style="list-style-type: none"> 1) In the Identities list, select the remote identity that you want to modify. The properties of the selected remote identity appear on the right. 2) Modify the properties of the remote identity as appropriate, then save your changes.

Task	Steps
Delete a remote identity	<ol style="list-style-type: none"> 1) In the Identities list, select the remote identity that you want to delete. 2) Click Delete. A confirmation pop-up window appears. 3) Click Yes, then save your changes.

Managing keys

Sidewinder keys are public/private key pairs that are used to perform public key cryptography for SSL and SSH content inspection.

During installation, these keys are uniquely generated:

- 2048 bit RSA
- 1024 bit DSA
- 2048 bit DSA


Services that use DSA are configured to use the 1024 bit DSA key.

To manage keys, select **Maintenance > Certificate/Key Management**, then click the **Keys** tab.

The following table lists the available keys. The Fingerprint is a hashed (shortened) version of the key that allows users to compare keys more easily.

Use the toolbar to perform these actions:

Table 112: Keys tab toolbar

Button	Action
New	Create a new key by clicking New and entering the key's properties in the pop-up window.
Delete	<p>Delete a key by selecting a key from the table and clicking Delete.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Note: Either the <code>Default_DSA_Key</code> or the <code>Default_RSA_Key</code> must exist in order to create a new SSH Application Defense. </div>
Import Key	Import a key generated on another device by clicking Import Key and then entering the key properties in the pop-up window.

Button	Action
Export Key	<ol style="list-style-type: none"> 1) Select the key you want to export. 2) Click Export Key. The Keys: Export Key window appears. 3) Specify an export destination, then click OK.

Related tasks

[Create a key](#) on page 635

[Import a key](#) on page 636

[Export a key](#) on page 636

Create a key

Create a new key for use in SSH or SSL connections.

Steps

1) Select **Maintenance > Certificate/Key Management**.

2) Select the **Keys** tab. The **Keys** tab appears.



Tip: For option descriptions, click **Help**.

3) Click **New**. The **Create New Key** window appears.

4) In the **Key name** field, enter a name to identify this key.

5) From the **Key type** drop-down list, select a key type.

6) From the **Key length** drop-down list, select a key length.



Note: Longer keys are more secure, but they can take longer to generate. They can slow down the establishment of encrypted communication channels. We recommend using keys that are at least 2048 bits long.

7) Click **Add** and save your changes.

Import a key

Import a key that was generated on another device.

Steps

1) Select **Maintenance > Certificate/Key Management**.

2) Select the **Keys** tab. The **Keys** tab appears.



Tip: For option descriptions, click **Help**.

3) Click **Import Key**. The **Import Key** window appears.

4) From the **Import source** drop-down list, select the source location of the key.

- **File** — Manually specify the location of the key
- **Cut and paste** — Import the key by cutting and pasting the key in the **Paste key here** box

5) In the **Key name** field, type a local name for the key you are importing.

6) [File source only] In the **Import key from file** field, type the name and location of the key to import, or click **Browse** to browse the network directories for the location.



Note: Binary (PKCS1) and PEM (PKCS8) file formats are supported.

7) [Cut and paste source only] In the **Paste key here** box, paste the key that you copied from the source.

8) Click **OK** to import the key.

9) Save your changes.

Export a key

Export a key to install on another device.

Steps

1) Select **Maintenance > Certificate/Key Management**.

2) Select the **Keys** tab. The **Keys** tab appears.



Tip: For option descriptions, click **Help**.

3) Click **Export Key**. The **Export Key** window appears.

4) Select the export destination:

- **Export key to file** — Export the key to a file

- **Export key to screen** — Export the key to a **Certificate Data** window, then cut and paste the key in the client

5) [Export to file only] Enter the file information.

- In the **File** field, type the name and location of the file to write the key to. If you want to overwrite an existing file but are not certain of the path name or the file name, click **Browse**.
- From the **Format** drop-down list, select the appropriate format for the file.



CAUTION: The private key is not protected when it is exported. If you use a transportable medium to store the private key file, the medium should be destroyed or reformatted after the private key information has been imported on the appropriate device.

6) Click **OK** to export the key to the desired location.

High Availability

Contents

- [How High Availability works](#) on page 639
- [HA configuration options](#) on page 641
- [Configuring HA](#) on page 644
- [Understanding the HA cluster tree structure](#) on page 649
- [Managing an HA cluster](#) on page 651

Two firewalls can be configured to work together to provide load sharing or redundancy. This configuration is known as a High Availability (HA) cluster.

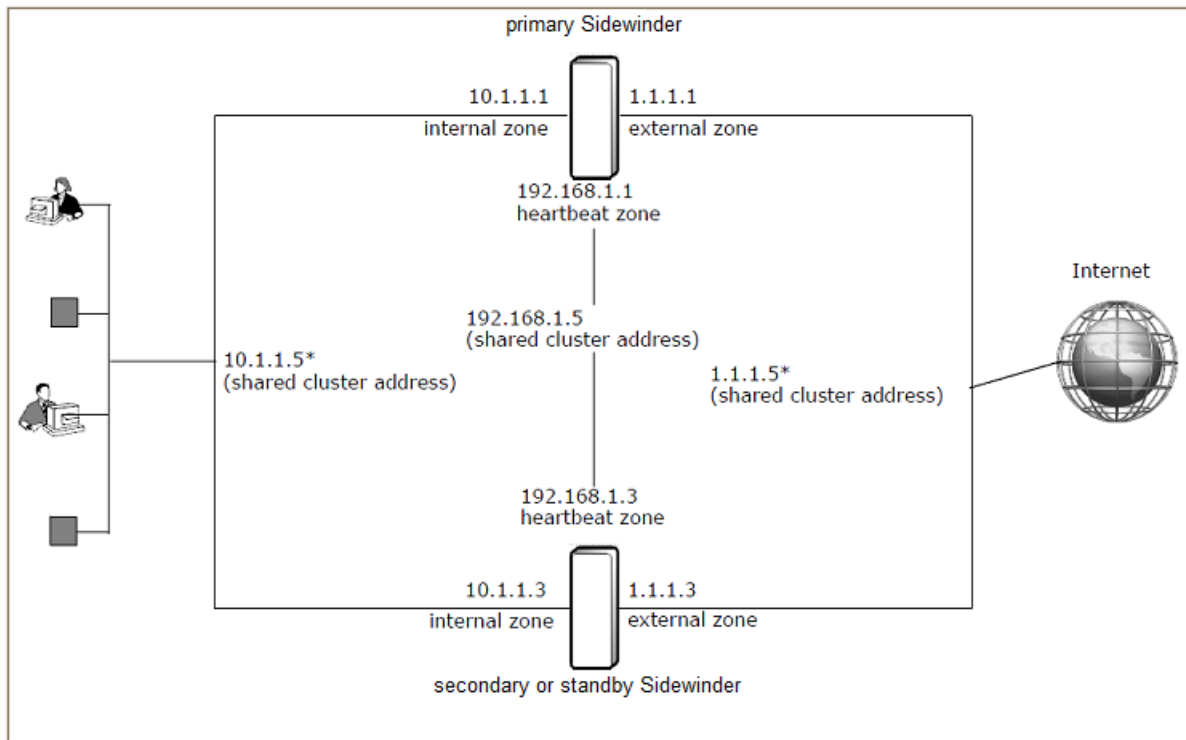
How High Availability works

HA clusters can be configured in load sharing or failover modes.

- **Load sharing** — Both the *primary* and *secondary* firewall actively process traffic, providing improved performance and redundancy.
- **Failover** — The *standby* firewall does not process traffic unless called on to take over if the primary becomes unavailable, providing redundancy.

As shown in the following figure, configuring an HA cluster requires at least three zones for each firewall: an internal zone, an external zone, and a heartbeat zone. The heartbeat zone isolates all HA cluster-specific traffic between the cluster firewalls so that it does not impact regular network traffic.

Figure 80: Basic HA configuration



To implement an HA cluster in your network, cluster firewalls must have interfaces that reside in the same networks and you need one additional shared cluster address for each network. This address represents the HA cluster rather than an individual firewall interface.

The following table summarizes the IP addresses needed for this HA configuration.

Table 113: HA IP addresses

	internal zone	external zone	heartbeat zone
primary IP	10.1.1.1	1.1.1.1	192.168.1.1
secondary/standby IP	10.1.1.3	1.1.1.3	192.168.1.3
shared cluster address	10.1.1.5*	1.1.1.5*	192.168.1.5*

* In a load sharing HA cluster, the shared cluster addresses (except the heartbeat) are shared between firewalls. In a failover HA cluster, they are assigned to the primary firewall.

In this example, all users in the internal or external network must use the cluster address (10.1.1.5 or 1.1.1.5, respectively) as the network gateway. Only system administrators should know about the other IP addresses. The same concept applies for DNS host names.



Tip: When configuring an existing single firewall to become an HA cluster, consider using the existing interface addresses as the cluster addresses and using new IP addresses for the actual NICs. This makes the transition from a single firewall to an HA cluster transparent to the rest of your network.

Handling failures

The two HA firewalls communicate on the heartbeat zone. An IPsec-authenticated heartbeat is sent by the primary and acknowledged by the secondary/standby.

Failures are handled as follows:

- **Load sharing HA** — If the primary or the secondary firewall becomes unavailable (that is, a heartbeat message or acknowledgment is not received from that firewall for the specified amount of time), the remaining firewall takes over and assumes responsibility for processing all traffic.
- **Failover HA** — If the standby determines that the primary is unavailable, the standby takes over and assumes the role of the primary and the responsibility for processing all traffic.

What HA clusters use

HA clusters use shared IP addresses to receive and transmit network traffic—to other hosts on the network, the HA cluster appears to function as a single firewall.



Note: The individual IP addresses of the firewalls are used for administration purposes only and should not be used to pass traffic.

HA and IPv6 support

Failover HA supports IPv6 addresses for all cluster interfaces except the heartbeat. Each non-heartbeat cluster interface supports IPv4 addresses, IPv6 addresses, or both.



Note: Load sharing HA does not support IPv6.

The following restrictions apply:

- For each shared IPv6 address, cluster firewalls must be assigned an individual IPv6 address in the same scope.
- The heartbeat and backup heartbeat interface must use IPv4 addresses. IPv6 addresses are not supported.

HA configuration options

You can configure HA clusters for load sharing or failover mode.

- **Load sharing** — Both the primary and secondary firewall actively process traffic.
- **Failover** — The standby does not process traffic unless called on to take over if the primary becomes unavailable.

Related concepts

[Load sharing HA](#) on page 642

[Failover HA](#) on page 643

Load sharing HA

Load sharing HA, also referred to as active-active HA, consists of two firewalls that actively process traffic in a load sharing capacity. When a secondary is registered to an HA cluster, synchronized areas are overwritten to match the primary.



Note: To configure load sharing HA, both firewalls must have the same hardware configuration (for example, CPU speed, memory, active NICs).

Load sharing HA provides the following benefits:

- **Performance** — Both firewalls actively participate in passing network traffic, which increases performance, especially in heavier workloads.
- **Redundancy** — Load sharing HA provides the same redundancy benefits as failover HA — if one firewall encounters a failure, the other firewall assumes responsibility for all traffic.
- **Outage transparency** — Load sharing HA masks outages from your users:
 - If a failover event occurs on one of the firewalls, the outage does not affect the active connections being handled by the operational firewall.
 - If you need to shut down a firewall, you can schedule a soft shutdown, which reduces the number of sessions that are lost.

Related concepts

[Managing an HA cluster](#) on page 651

How load sharing HA works

Each network interface on both firewalls maintains an individual IP address and shared cluster address(es) with one exception: only the primary is assigned the cluster address for the heartbeat zone.

The firewalls share the cluster IP addresses using one of several configurable layer 2 modes, allowing them both to receive all traffic sent to the shared cluster addresses. The communication to coordinate load sharing passes between firewalls on the heartbeat zone.

The firewalls determine how to balance the load by examining the source port of incoming connections' one firewall processes the incoming connections with even source ports while the other firewall processes the incoming connections with odd source ports. However, the following types of traffic are always processed by the primary firewall:

- All management traffic, such as Admin Console, SSH, Telnet, and SNMP
- VPN
- ICMP
- Any other type of traffic that does not include a source port

Once a connection is processed by one of the cluster firewalls, all of the packets associated with that connection are handled by the same firewall. Connections that are specifically addressed to an individual firewall address will be assigned to the specified firewall.

To share the cluster IP addresses, firewalls that are configured for load sharing HA use a common cluster MAC address for each cluster interface. To accommodate varying switch capabilities, load sharing clusters can be configured to use one of the following layer 2 modes:



Note: For more information on the available layer 2 modes and the configuration requirements these modes present for your switches and/or routers, see Knowledge Base article [8877](#).

- **Unicast - mirrored** — In this mode, each cluster interface on both firewalls is assigned a shared unicast MAC address. Because a unicast MAC address normally corresponds to a single host, the cluster firewalls rely on switches to forward traffic destined for a cluster MAC address to both cluster firewalls. To accomplish this, each switch that is connected to the cluster firewalls must be configured to send traffic destined for the unicast cluster MAC address to both firewall interfaces.
- **Multicast** — In this mode, each cluster interface on both firewalls is assigned a shared multicast MAC address. If you select this mode and your routers have difficulty processing ARP replies that contain multicast MAC addresses, add static ARP entries on the routers.



Note: This mode uses layer 2 multicast, which should not be confused with IP multicast (which functions at layer 3).

- **Unicast - flooded** — In this mode, each cluster interface on both firewalls is assigned a shared unicast MAC address. This mode differs from Unicast - mirrored mode because it does not require any special configuration on your switches. Instead, the firewalls prevent each switch from establishing an association between the cluster MAC address and the switch port on which it can be reached. This causes each switch to send all Ethernet frames destined for the cluster MAC address out all of its ports, allowing both firewalls to receive Ethernet frames destined for the cluster MAC address.



Note: This mode is useful if the switches that are connected to the cluster firewalls do not support Multicast mode or Unicast - mirrored mode. However, this mode increases network overhead for all devices that are connected to the switch.

Soft shutdown

If you know in advance that a firewall will need to be shut down, you can reduce the number of lost connections by scheduling the shutdown (rather than shutting down immediately).

When a shutdown is scheduled for a later time, a soft shutdown will be performed to reduce the number of sessions that are lost.

Related concepts

[Scheduling a soft shutdown for a load sharing HA cluster Sidewinder](#) on page 657

Failover HA

Failover HA consists of one firewall (the primary) actively processing traffic with the standby acting as a hot backup. When a standby firewall is registered to an HA cluster, synchronized areas are overwritten by the HA cluster configuration.

When the primary is brought online, it activates its individual interface addresses, the cluster addresses, and any aliases assigned to the cluster. When the standby is brought online, it activates only its individual interface IP addresses.

If the standby does not receive a heartbeat signal for a number of seconds (based on the takeover setting of the standby), it activates the shared cluster addresses on its interfaces and begins processing network traffic. In the process, the standby clears its address resolution protocol (ARP) cache and attempts to generate a *gratuitous ARP*.

Most systems will immediately determine that the standby is now responsible for the addresses the primary is known by (the cluster addresses), and new connections will be established through the new acting primary. However, there might be a number of reasons why the gratuitous ARP is not received: a remote system might not recognize the message, the message might be blocked by certain switches or it might fail due to timing issues. This can often be resolved by performing one of these options:

- Flushing the ARP cache on the remote system.
- Shortening the time that entries stay in the remote system ARP cache to 3–5 minutes.
- Configuring systems to communicate with the new ARP address by selecting the **Force ARP Reset** option on the **High Availability Advanced Network Properties** window when creating an HA cluster.

You can configure failover HA in one of two ways:

- **peer-to-peer** — In a peer-to-peer HA cluster, both firewalls are configured as standbys with the same takeover time. The first firewall to come online becomes the primary. If the primary becomes unavailable, the peer, currently acting as the standby, takes over as the primary. This firewall remains the primary until it becomes unavailable, at which time the peer takes over as the acting primary. This is the recommended failover HA configuration. However, to configure peer-to-peer HA, both firewalls must have the same hardware configuration.
- **primary/standby** — In a primary/standby HA cluster, one firewall is designated as the primary and always acts as the primary when it is available. The standby firewall takes over as the acting primary only if the designated primary becomes unavailable. When the primary firewall recovers and becomes available, it resumes its role and another takeover event occurs. This additional takeover event does not occur in a peer-to-peer configuration. Use this option if you have firewalls that do not share the same hardware configuration, using the firewall with higher performing hardware as the primary.



Note: When a takeover event occurs, a number of netprobe events can be detected when connections take time to detect the switch of systems.

Failover HA provides the following benefits:

- **Redundancy** — The standby firewall acts as a hot standby, ready to take over if the primary becomes unavailable.
- **Simple configuration** — Failover HA requires less configuration on your switches and/or routers than load sharing HA.
- **Flexible hardware requirements** — The requirements for failover HA are less stringent than load sharing HA.
 - If your firewalls have similar hardware configurations but do not meet the requirements for load sharing, you can configure them for peer-to-peer HA.
 - If your firewalls have mismatched hardware, you can configure them for primary/standby HA.

Configuring HA

This section provides the basic information you need to configure an HA cluster.

Before you begin, sketch a diagram showing your planned configuration for reference. Include the following items on your diagram:

- Interfaces
- IP addresses
- HA shared cluster addresses
- Zone names

Perform these procedures to create an HA cluster:

- 1) Gather HA requirements

- 2) Configure the heartbeat interfaces
- 3) Add the first Sidewinder to a new HA cluster
- 4) Add a reservation for the second firewall in the HA cluster
- 5) Join a Sidewinder to an existing HA cluster



Note: A configuration backup is automatically performed and stored on the Sidewinder when creating an HA cluster.

HA requirements

Before you configure HA, the following conditions must be met.

- Both firewalls must be at the same version.
- The same administrator user account must exist on both firewalls.
- A dedicated heartbeat zone and interface must be configured on each firewall. We recommend directly connecting the heartbeat interfaces using these types of cables:
 - **100baseT NIC** — Crossover cable
 - **1000baseTX NIC** — Cat5e or Cat6 cable
 - **1G or 10G NIC** — Appropriate fiber optic cable



Note: If the heartbeat interfaces are connected through a switch, that switch must be configured to pass IGMP, and cannot decrement the Time To Live (TTL).

- SPAN and transparent interfaces must be disabled or deleted.
- The following areas must be configured identically:
 - Number and types of interfaces
 - Number of zones
 - Zone names (case-sensitive)
 - Zone creation order



Note: You can verify the order zones were created in by running the `region` command at the command line. The output from this command must match on both firewalls.

Additional requirements for load sharing clusters

Before you configure load sharing HA, the following additional requirements must be met.

- The Sidewinder appliances must have identical hardware configuration.
- The interface used for the heartbeat zone must be at least as fast as the fastest load sharing interfaces on your firewall.
- The switches connected to your firewalls must meet certain requirements depending on the layer 2 mode you configure for the cluster.

- The unicast - mirrored and unicast - flooded layer 2 modes are supported only on em and igb NICs, including the 1 Gbps ports on S model appliances.
- If VLAN interfaces that share the same parent NIC or NIC group are configured to use either the Unicast - mirrored or Unicast - flooded layer 2 modes, they must meet the following requirements:
- They must share the same cluster MAC address
- They must use the same layer 2 mode (Unicast - mirrored or Unicast - flooded)



Note: A load sharing HA cluster enforces these requirements, keeping the cluster MAC address and layer 2 mode of the appropriate VLAN interfaces synchronized.

Related concepts

[How load sharing HA works](#) on page 642

Related tasks

[Configure the heartbeat interfaces](#) on page 646

Configure the heartbeat interfaces

You must configure a dedicated heartbeat zone and interface on each firewall *before* configuring an HA cluster. To configure the heartbeat interfaces, follow the steps below.

Steps

- 1) Ensure that each firewall has an interface that can be dedicated to HA traffic.



Note: Do not use a VLAN for the heartbeat zone.

- 2) In the Admin Console, connect to one of the firewalls and create a heartbeat zone.
 - a) Select **Network > Zone Configuration**.
 - b) Click **New**.



Tip: For option descriptions, click **Help**.

- c) Type a name and optional description for the heartbeat zone.
 - d) Select the **Respond to ICMP echo and timestamp** check box.

Note: Do not select **Hide port unreachable** for a heartbeat zone.
 - e) Click **OK** and save your changes.
- 3) Select **Network > Interfaces** and select the heartbeat zone for an existing interface or create a new interface that includes the heartbeat zone.
 - 4) Save your changes.

- 5) Repeat these steps *Step 1* through *Step 4* for the other firewall that will be participating in the HA cluster.
- 6) Connect the heartbeat zones with the appropriate cable.
 - **100baseT NIC** — Use a crossover cable.
 - **1000baseTX NIC** — Use a standard Cat5e or Cat6 cable.
 - **1G or 10G NIC** — Use an appropriate fiber optic cable.
- 7) Test the network connectivity between the two firewalls for the heartbeat interface.



Note: Network connectivity must exist between the heartbeat zones to successfully configure HA.

Add the first Sidewinder to a new HA cluster

Use the **Cluster Wizard** to add the first firewall to a new HA cluster.

Steps

- 1) In the Admin Console, connect to the firewall that will become the primary.
- 2) Verify that you have a dedicated heartbeat zone and interface configured for HA on this firewall.
- 3) Select **Maintenance > Cluster Wizard**.
- 4) Click **Launch Cluster Wizard**.
The **Cluster Wizard** window appears.



Tip: For option descriptions, click **Help**.

- 5) Click **Next**.
The **Create New or Join Existing Cluster** page appears.
- 6) Select **Create New Cluster**, then click **Next**.
- 7) Follow the wizard to complete the process.

Add a reservation for the second firewall in the HA cluster

Before joining a Sidewinder to an existing HA cluster, you must make a reservation for that firewall in the **High Availability** window of the HA cluster.

Once you have *added* the firewall to the HA cluster, you will need to *join* the firewall to the HA cluster using the **Cluster Wizard**.

Use the **High Availability** window to add a reservation for the new firewall in the existing HA cluster.

Steps

- 1) Connect to the HA cluster IP address using the Admin Console.
- 2) In the **Admin Console** tree, select **High Availability**.
The **High Availability** window appears.
- 3) In the **Pair Members** area, click **New**.
The **Add New Firewall** window appears.
- 4) In the **Hostname** field, enter the name of the firewall you are adding to the HA cluster. The name must be a fully qualified host name in the same domain as the primary.
- 5) [Primary/standby only] In the **Takeover Time** field, select the number of seconds that the primary must be unavailable before the secondary/standby will begin the takeover process. The default value is **13** seconds.
- 6) In the **IP Address in Heartbeat Zone** field, enter the individual IP address (in the heartbeat zone) of the firewall that you are adding to the HA cluster.
- 7) In the **Registration Key** field, create the registration key for this HA cluster. The key must be at least one character long and may consist of alphanumeric characters, hyphens (-), and underscores (_).



Tip: For option descriptions, click **Help**.



Note: You will need the registration key when you join the firewall to the HA cluster using the **Cluster Wizard**. Click **Add** to add the firewall to the HA cluster.

Result

You can now join the Sidewinder to the HA cluster using the **Cluster Wizard**.

Join a Sidewinder to an existing HA cluster

Use the **Cluster Wizard** to join a firewall to an existing HA cluster.

Steps

- 1) Using the Admin Console, connect to the firewall that will be joining the HA cluster.
- 2) Select **Maintenance > Cluster Wizard**.
- 3) Click **Launch Cluster Wizard**. The **Welcome** window appears.
- 4) Click **Next**. The **Create New or Join Existing Cluster** page appears.
- 5) Select **Join Existing Cluster** and then click **Next**.



Tip: For option descriptions, click **Help**.

- 6) Follow the wizard to complete the process.

Understanding the HA cluster tree structure

The Admin Console tree structure is slightly different for an HA cluster. When you administer an HA cluster, both firewalls are managed within a single Admin Console connection to the cluster IP address.

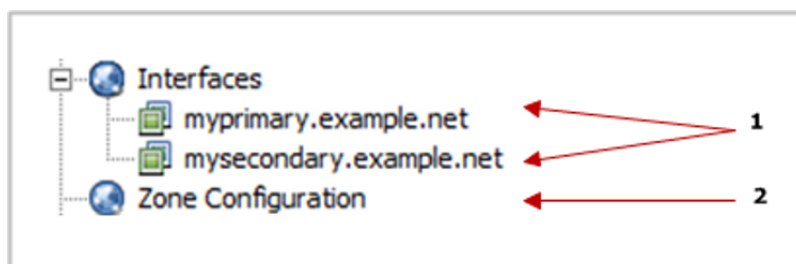
Areas of the HA cluster that are synchronized (that is, areas in which the information for both firewalls must be the same and remains in sync) will appear with a single tree option. When you modify information within those areas, the information will automatically be updated for both firewalls.

Information specific to individual firewalls within the HA cluster (such as configuration backup and restore) includes a sub-folder (indicated by a plus[+] sign) that contains an icon for each firewall that is part of the HA cluster. To modify information within these areas, expand the tree branch, select the appropriate firewall, and make the desired changes. Non-synchronized modifications to an individual firewall will be applied only to that firewall and will not be overwritten by changes made to the other firewall.

The **License** window is further split in an HA cluster: The **Contact** and **Company** tabs appear when you select **License** in the tree; the **Firewall** and **Enrollment List** tabs appear when you select an individual Sidewinder.

The figure demonstrates the difference between an individually configured area of the HA cluster (Interfaces) and a synchronized area of the HA cluster (Zone Configuration).

Figure 81: Example of an individually configured area



- 1) Interfaces are configured on an individual firewall basis.
- 2) Zone Configuration is synchronized, and does not allow you to select an individual firewall.

The **Date and Time** and **License** areas within the HA cluster tree include some areas that are synchronized and some areas that are configured on an individual firewall basis, as shown in the figure.

Figure 82: Date and Time and License areas

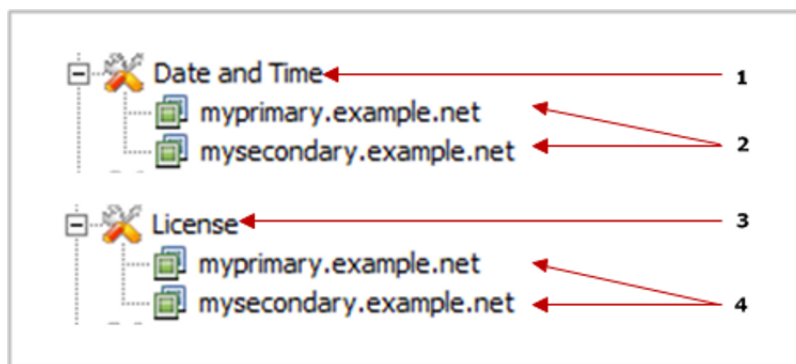


Table 114:

- 1) Synchronized time zone and time synchronization information is configured by selecting the main Date and Time option.
- 2) System clock information specific to a single firewall is configured by selecting that firewall.
- 3) Synchronized contact and company information is configured by selecting the main License option.
- 4) The serial number and host enrollment list specific to a single firewall is configured by selecting that firewall.

Synchronized features

The following features are synchronized within an HA cluster.

- Administrator Accounts
- Application Defenses
- Attack Responses
- Audit Management
- DHCP Relay
- DNS
- High Availability
- Shared Interface Addresses
- Network Defenses
- Routing
- Rules
- Rule Elements
- sendmail
- System Responses
- VPN Configuration
- Zone Configuration

Individually managed features

The following features are managed individually within an HA cluster.

- Dashboard
- Interfaces
- Configuration Backup
- Date and Time
- Audit Viewing
- License
- Software Management
- System Shutdown
- File Editor
- Hardware Acceleration

Managing an HA cluster

When you have configured an HA cluster, the HA cluster will be represented in the Admin Console tree by one combined firewall icon.

When you connect to the HA cluster, you will use the HA shared cluster address that you created when you configured HA. This allows you to manage both firewalls by connecting to the HA cluster.

Modifying HA common parameters

Use the **High Availability** window to configure properties that are common to the HA cluster.

These parameters affect all firewalls in your HA configuration. These properties were set when you ran the **Cluster Wizard** (if you skipped the advanced properties windows, many of these properties were set automatically).



Note: If you make any configuration changes on this window, both cluster firewalls must be restarted.

Related tasks

[Restart an HA cluster](#) on page 658

Configure or modify common HA parameters

Configure common HA parameters.

Steps

- 1) From the Admin Console, connect to the HA cluster.

- 2) In the Admin Console tree, select **High Availability**. The **High Availability** window appears.



Tip: For option descriptions, click **Help**.

You can configure or modify the following areas:

High Availability Identification

The firewall depends on several items for identification in High Availability.

- **Cluster ID** — The default value does not require modification; valid values are 1–255. If modified, each firewall within an HA cluster must be assigned the same cluster ID.
- **Multicast Group Address** — Displays the address of the multicast group used for HA purposes on the heartbeat zone. The default address is 239.255.0.1. To modify the address, click **Edit address**.
 - Do not specify an address that conflicts with other multicast groups on the heartbeat zone. Addresses in the range of 239.192.0.0 to 239.255.255.255 have been reserved by RFC 2365 for locally administered multicast addresses.
 - Boundary routers should be configured to not pass your selected address if such a feature exists.



Note: If the default is not used, you should change the reverse lookup files in DNS to allow DNS reverse resolution of the multicast address. Refer to the `/etc/namedb.u/failover.rev` file.

- **Heartbeat Zone** — Displays the zone that HA uses to send or receive a heartbeat. A *heartbeat* is a short message that is sent out at specific intervals to verify whether a Sidewinder is operational. The heartbeat, session information, and configuration information are also transferred between the heartbeat zones. This must be a dedicated heartbeat zone.

To change the heartbeat zone, select a new one from the drop-down list.



Note: In rare circumstances, if the heartbeat zone needs to be modified, consult with the Support team.

- **Heartbeat Verification Zone** — From the drop-down list, select the zone that HA will use to send or receive a mini-heartbeat. This should be a zone that regularly passes traffic, such as the internal zone. This mini-heartbeat helps protect against false failover events by doing the following:

- If the firewall does not detect the heartbeat but does detect the mini-heartbeat, the HA cluster does not fail over. An audit message is generated, alerting the administrator to check the heartbeat zones' connectivity.

Loss of communications on the heartbeat zone causes diminished HA services.

- For load sharing HA, the active secondary no longer shares the session load; it goes to a standby state.
- For failover HA, the standby cannot receive updated information about new packet filter sessions established on the primary.
- If the firewall does not detect either the heartbeat or the mini-heartbeat, the HA cluster fails over.

Additional information on heartbeat verification is available in Knowledge Base article [8851](#).

IPSec Authentication Password

This field displays the auto-generated password that is used to generate the authentication key for IPsec. You should not change this password.

Pair Members

The **Pair Members** table lists the firewalls that are in the HA cluster.

- If one firewall is in the list, you can perform these actions:
 - Click **New** to add the second firewall to the cluster. This reserves a space in the cluster for the second firewall. You must then join the second firewall to the cluster.
 - Click **Change State to Standalone** to remove the primary firewall from the HA cluster.
- If two firewalls are in the list, you can perform these actions:
 - Select the standby and click **Delete** to remove the standby firewall from the cluster.
 - Click **Cluster Status** to see which firewall is the current primary and which is the secondary.
- **Auto-Recover On Reconnect** — When a monitored interface fails, it triggers a failover event that causes the primary firewall to become a standby firewall. The **Auto-Recover On Reconnect** checkbox controls how the standby firewall returns to the cluster once the connection is restored.



Note: The **Auto-Recover On Reconnect** option only applies to peer-to-peer and primary/standby HA configurations.

The effects of the **Auto-Recover On Reconnect** option are summarized in the following table.

Table 115: Auto-Recover on Reconnect summary

HA cluster configuration	Auto-Reconnect on Recover checkbox is...	
	Selected	Deselected
Peer-to-peer	The standby firewall is available for failover when the monitored interface reconnects.	An administrator must manually restart the standby node in order to make it available for failover.
Primary/standby	The standby firewall will return as the cluster primary when the monitored interface reconnects.	An administrator must manually restart the standby node in order to restore it to the cluster as the primary firewall.
Load sharing	No effect	No effect

The remote test IP addresses that monitor interfaces are displayed and configured through the **Cluster Interfaces** table.

Related tasks

[Add a reservation for the second firewall in the HA cluster](#) on page 647

[Join a Sidewinder to an existing HA cluster](#) on page 648

Type

Use the **type** area to change the type of the High Availability cluster.

Options are:

- **Load-sharing**
- **Peer-to-peer**
- **Primary/Standby**

If you select **Primary/Standby**:

- 1) Use the **Cluster Primary** field to select one of the cluster members to serve as the primary.
- 2) In the **Cluster Takeover** field, select a time in seconds to wait before the standby firewall becomes primary.

Modify cluster interface properties

Use the **Cluster Interface Properties** window to perform the following actions.

- Create, modify, or delete remote test IP addresses.
- Create, modify, or delete force ARP reset IP addresses.

To access the **Cluster Properties Interface** window:

Steps

- 1) Select **Network > Interfaces**, and select the firewall you want to modify. The **Interface Configuration** tab appears.



Tip: For option descriptions, click **Help**.

- 2) Select an interface, then click **Modify**. The **Interface Properties** window appears.
- 3) Click **Advanced Cluster Settings**. The **Cluster Interface Properties** window appears.

[Load sharing only] Change the layer 2 mode

If the switch that is connected to this interface does not support the layer 2 mode that is currently configured, select a different mode from the **L2 Mode** drop-down list.

- **Unicast - mirrored** — Select this mode if the switch that is connected to this interface can be configured to send traffic destined for single unicast MAC addresses out multiple ports.
- **Multicast** — Select this mode if the switch that is connected to this interface does not support Unicast - mirrored mode but does support multicast MAC addresses.
- **Multicast no IGMP** — Select this mode if the switch that is connected to this interface supports multicast MAC addresses and you do not want this interface to send IGMP messages advertising the cluster MAC address. This is the layer 2 mode used by load sharing HA clusters at version 7.0.0.07 and earlier. Only select this mode if you must do so to preserve compatibility with the switch that is connected to this interface.
- **Unicast - flooded** — Select this mode if the switch that is connected to this interface does not support Multicast mode or Unicast - mirrored mode.

For more information on the available layer 2 modes and the configuration requirements these modes present for your switches and/or routers, see:

- How load sharing HA works
- Knowledge Base article [8877](#)

Related concepts

[How load sharing HA works](#) on page 642

[Load sharing only] Change the cluster MAC address

Change the cluster MAC address by editing the **Cluster MAC** field.

- Do not modify the cluster MAC address unless it conflicts with a device that is attached to the same network or you are instructed to do so by [Forcepoint support](#).
- Do not change the first three octets (xx:xx:xx:yy:yy:yy) of the cluster MAC address.

Monitor the interface link

Test whether the interface link is active by selecting **Monitor link status**. This checks if the interface is disconnected or the NIC stops working. It does not verify that other devices can be contacted by the firewall.

Create, modify, or delete remote IP addresses for Interface Test

In the **Interface Test** area, configure remote test IP addresses for networks that you want to periodically ping. Ping addresses must be in highly reliable systems that are directly attached to the Sidewinder network.

Steps

- 1) Click **New**, then click the **Specify IP Address** field and type an IP address that the firewall will ping.



Tip: For option descriptions, click **Help**.

- 2) In the **Ping interval** field, specify how often (in seconds) the firewall will ping the remote address to ensure that an interface and path are operational.

- 3) In the **Failures allowed** field, specify the number of failed ping attempts that must occur before the standby interface takes over as the primary.

Failures are counted in increments and decrements rather than successively. This means that a failed ping adds to the failure total, and a successful ping subtracts from the failure total. The failure total is never less than zero and it is never more than the configured failures allowed.

For example, if the configured failures allowed is 3, this is how the failure count is tallied based on the ping results:

Table 116: Example ping results

Ping result:	failure	success	success	failure	failure	success	failure	failure	<i>Failover event occurs</i>
Failure total:	1	0	0	1	2	1	2	3	

- To modify a ping IP address, double-click the address in the list and make the change.
- To delete a ping IP address, select it in the list and click **Delete**.



Note: If the primary becomes unavailable immediately after a ping attempt has been issued, the time it takes for a secondary/standby to take over will be slightly longer (this is because it will take close to an entire test interval before the first failure is detected).

[Failover HA only] Create, modify, or delete IP addresses for Force ARP Reset

In the **Force ARP Reset** area, configure hosts that are known to ignore gratuitous ARPs, but that need to know the new cluster alias.

Click **New**, then click the **Specify IP Address** field and type an IP address that will not respect gratuitous ARP requests.

- To modify an entry, double-click the address in the list and make the change.
- To delete an entry, select it in the list and click **Delete**.

[IPv6 only] Create, modify, or delete IP addresses for Force NDP Reset

In the **Force NDP Reset** area, configure devices that ignore NDP commands during a failover event. The HA cluster attempts to force devices that ignore NDP commands to update their NDP tables.

Click **New**, then click the **Specify IP Address** field and type an IP address that will not respect NDP commands.

Scheduling a soft shutdown for a load sharing HA cluster Sidewinder

When a Sidewinder that belongs to an HA cluster is shutdown by an administrator (for example, to perform scheduled maintenance), a *soft shutdown* will automatically occur (assuming the shutdown time is not immediate).

A soft shutdown provides a buffer period before the actual shutdown occurs, allowing the firewall to stop accepting new connections, while allowing most existing connections to complete before the firewall actually shuts down. IP packet filter processing is also transferred to the remaining firewall.



Note: A peer must be available in order to perform a soft shutdown.

By default, the soft shutdown process will begin 30 minutes prior to a scheduled shutdown. If the shutdown is scheduled to occur in less than 30 minutes, the soft shutdown process will begin immediately and will remain in effect until the actual shutdown time occurs. You can also manually increase or decrease the length of the soft shutdown period.

For example, suppose you configure the firewall to shutdown in two hours using the default soft shutdown of 30 minutes. The firewall continues to accept and process connections for 1.5 hours. When the firewall is 30 minutes from the shutdown time, it stops accepting new connections (the other firewall processes all new connections). Existing connections will have 30 minutes to complete. After the soft shutdown period completes, the firewall will shut down and will be unavailable until it is restarted.

The soft shutdown feature is specified via command line. If you schedule a shutdown using the Admin Console, the default soft shutdown time will be applied. The following bullets provide examples of configuring an HA cluster firewall for shutdown:

- If you want the soft shutdown process to begin immediately, use the following command (the firewall must be shut down or manually restarted once the soft shutdown process is complete):

```
cf cluster softshutdown
```

- To configure soft shutdown to occur for a specific amount of time, as follows:

```
shutdown -s [soft_shutdown_time] [shutdown_time]
```

The *soft_shutdown_time* specifies that amount of time that soft shutdown will occur. The *shutdown_time* specifies the time at which the actual shutdown will occur. Each variable can be specified either as a number of minutes or as an exact date and time. If you are specifying the number of minutes, you must include a plus (+) sign in front of the minutes.

For example, if you want the firewall to shut down on Saturday, June 12, 2004 at 11:00 am with a 15 minute soft shutdown period, you would enter the following command:

```
shutdown -s +15 0406121100
```

In this case, the soft shutdown process would begin at 10:45 am, and the firewall would shutdown at 11:00 am on the specified day.

If you want the firewall to begin the soft shutdown at 6:00 am with an actual shutdown at 6:20 am, you would enter the following command:

```
shutdown -s 0600 0620
```



Note: For a complete listing of shutdown options, refer to the shutdown man page.

You can cancel a scheduled shutdown at anytime prior to the final 30 minute period by entering the `shutdown -c` command. However, once the firewall has entered soft shutdown mode, this command will no longer cancel the soft shutdown process. When the soft shutdown process is complete, you will need to restart the firewall before it will properly function as part of the HA cluster.

Re-establish an HA cluster if a cluster member fails

If a member of an HA cluster is no longer functional and must be re-installed, you can re-establish the cluster by restoring a configuration backup. You can use the configuration backup from either the failed cluster member or the remaining cluster member.

To re-establish an HA cluster:

Steps

- 1) Re-install the failed firewall or install a new system with the same host name.
- 2) Add the new or re-imaged firewall to the **Admin Console** tree.
- 3) Use the Admin Console to connect to the new or re-imaged firewall.
- 4) Restore the configuration file to the new system: Select **Maintenance > Configuration Backup**.



Tip: For option descriptions, click **Help**.

Result

The firewall restores to the configuration backup and then restarts. When it finishes starting, it rejoins the HA cluster.

Restart an HA cluster

If you make configuration changes to the **High Availability** window, you must restart both cluster firewalls.

To restart both firewalls in your HA cluster:

Steps

- 1) Shut down the secondary/standby:
 - a) Select **Maintenance > System Shutdown > secondary** icon.
 - b) Select **Halt System**.



Tip: For option descriptions, click **Help**.

- c) Select **Shutdown Immediately**.

- d) Click **Perform Shutdown**.
- 2) Shut down the primary:
 - a) Select **Maintenance > System Shutdown > primary icon**.
 - b) Select **Reboot to Operational Kernel**.
 - c) Select **Shutdown Immediately**.
 - d) Click **Perform Shutdown**.
 - 3) When the primary is finished restarting, start up the secondary/standby.

Enable and disable load sharing for an HA cluster

Change the mode of the HA cluster.



Tip: We recommend scheduling downtime to perform this procedure because it involves restarting both firewalls.

Steps

- 1) Connect to the HA cluster and select **High Availability**.
- 2) In the Type area, from the **Cluster Type** drop-down list, select a cluster type.
 - **Load-sharing** — Enable load sharing for the HA cluster (both firewalls actively process traffic).
 - **Peer to Peer** — Disable load sharing HA and convert the HA cluster to a peer-to-peer HA cluster (first firewall to come online becomes the primary firewall).
 - **Primary/Standby** — Disable load sharing HA and convert the HA cluster to a failover HA cluster (only one firewall processes traffic, with the other firewall acting as a backup). Select an option:
 - **Primary** — Make the selected icon the primary member of the cluster.
 - **Standby** — Make the selected icon the standby member of the cluster.



Tip: For option descriptions, click **Help**.

- 3) [Conditional] If you selected **Primary/Standby**, from the **Cluster Primary** drop-down list, select the firewall you want to be the primary firewall for the HA cluster.
- 4) [Optional] In the **Cluster Takeover Time** field, specify the number of seconds to wait before the secondary firewall takes over.
- 5) Save your changes.
- 6) Wait 60 seconds to allow the firewalls to synchronize.

- 7) Restart the cluster firewalls:
 - a) Shut down the secondary/standby.
 - b) Restart down the primary.
 - c) When the primary is finished restarting, start up the secondary/standby.

Related concepts

[Load sharing HA](#) on page 642

Related tasks

[Restart an HA cluster](#) on page 658

Remove a Sidewinder from an HA cluster

Use the appropriate task to remove a firewall from an HA cluster.

Related tasks

[Remove a secondary/standby from an HA cluster](#) on page 660

[Remove the primary from an HA cluster](#) on page 661

Remove a secondary/standby from an HA cluster

Change the secondary/standby firewall to a standalone firewall.

Steps

- 1) Connect to the HA cluster and select **High Availability** in the **Admin Console** tree. The **High Availability** window appears.



Tip: For option descriptions, click **Help**.

- 2) In the **Pair Members** table, select the secondary/standby and then click **Delete**.
When the firewall is removed from the HA cluster, it will transition to a standalone state.
- 3) To connect to the removed firewall, you must add it to the **Admin Console** tree:
 - a) From the **File** menu, select **New Firewall**. The **Add Firewall** window appears.
 - b) Enter the firewall name and IP address, then click **Add**.

Remove the primary from an HA cluster

You must remove the secondary/standby from the HA cluster before you can remove the primary from the HA cluster.

After you have removed the secondary/standby from an HA cluster, follow these steps to remove the primary from the HA cluster.

Steps

- 1) From the Admin Console, connect to the primary using the cluster address.
- 2) In the **Admin Console** tree, select **High Availability**. The **High Availability** window appears.



Tip: For option descriptions, click **Help**.

- 3) In the **Pair Members** area, click **Change State to Standalone**. The **Cluster Wizard Welcome** window appears.
- 4) Click **Next**.
- 5) Select **Change To Standalone**, and then click **Next**.
The **Cluster Wizard Summary** window appears.
- 6) Review the summary. When you are satisfied with the summary of changes, click **Execute** and then click **Yes**.
A progress bar appears while the configuration changes are made. If the transition is successful, the **Success** window appears displaying the new state.
- 7) Click **Finish**. The Admin Console disconnects. The firewall will transition to a standalone state.

Troubleshooting

Contents

- [Rules](#) on page 663
- [Determine functioning of HA](#) on page 672
- [Troubleshoot logon issues](#) on page 676
- [Check network status](#) on page 678
- [NTP](#) on page 684
- [Startup](#) on page 687
- [System status](#) on page 690
- [Troubleshooting transparent \(bridged\) mode](#) on page 692
- [Troubleshooting VPNs](#) on page 692
- [Contacting technical support](#) on page 692

Identify and resolve technical and configuration issues on your firewall.

Rules

This section includes troubleshooting information for the following.

Identify matched policy rules

You can review extra audit information to identify what rule acted on the connection.

The firewall `aconn` command helps you troubleshoot whether the connection is matching an access control rule, an SSL rule, or whether rules are being skipped.

From the command line, you can set the parameters of the connections to check traffic using a combination source IP address, destination IP address, port, or protocol. The command can be customized for specific traffic. The minimum parameter required to run the tool is either a source IP address or a destination IP address. The command does not affect existing sessions — only the new sessions. To run the tool with a different set of parameters, stop the command or restart the command line session.



Note: This tool is not available to read-only administrators.

Information is also available by typing `man aconn` at a firewall command prompt.

Policy troubleshooting scenario

With complex policy and large rule sets, it can be difficult to identify how a connection is processed. The policy troubleshooting tool provides information about which rule was matched.

Scenario: Assume that an employee in the Sales group has an IP address of 10.11.11.11 and is not able to connect to their AirAIM instant messaging service. Using the policy example below, you might expect that all employees in the sales group would be able to use the AirAIM application.

Table 117: Policy example

Name	Position	Source IP address	Destination IP address	Application	User/group
rule1	1	subnet:10.12.12.0	<Any>	AirAIM <ul style="list-style-type: none"> Port: 80/443 Protocol: TCP 	sales
rule2	2	<Any>	<Any>	FTP <ul style="list-style-type: none"> Port: 21 Protocol: TCP 	<Any>
rule3	3	<Any>	10.10.10.10	HTTP <ul style="list-style-type: none"> Port: 80/443 Protocol: TCP 	jsmith
rule4	4	10.11.11.11	<Any>	SSL/TLS <ul style="list-style-type: none"> Port: 443 Protocol: TCP 	<Any>
rule5	5	subnet:10.11.11.0	<Any>	AirAIM <ul style="list-style-type: none"> Port: 80/443 Protocol: TCP 	marketing
Deny All	6	<Any>	<Any>	<Any>	<Any>

To verify, we can apply the command:

```
aconn -s 10.11.11.11 -d 10.10.10.10 -p 80 -P tcp
```


This audit event would be the result:

```
2014-01-22 09:56:10 -0600 f_server a_server t_info p_minor
pid: 12654 logid: 100 cmd: 'aconn' hostname: firewall.exempl.net event: policy explain
srcip: 10.11.11.11 srcport: 58612 srczone: internal dstip: 10.10.10.10
dstport: 80 dstzone: external protocol: 6
reason: Detailed policy decisions for an incoming connection
information:
Matched SSL Rule 'Exempt All'
Skipped Rule 'rule1': Source (subnet:10.12.12.0) != 10.10.10.10
Skipped Rule 'rule3': Application != AirAIM
Skipped Rule 'rule5': Group != sales
Matched Rule 'Deny All'
```



Note: Rule2 and rule4 are not considered because they do not include port 80.

From the audit, you can see that the employee's IP address and user group did not match any of the allow rules. The Deny All rule caught the connection. To solve the issue, you could merge rule1 and rule5.

Run the policy troubleshooting tool

To see verbose audit entries related to policy rules, enter the parameters of the command.

Steps

- 1) From the command line, log on to the firewall.
- 2) Type `srole` to change to the Admin domain.
- 3) Type the command:

```
aconn -s <source IP> -d <destination IP> -p <destination port> -P <protocol>
```



Note: The minimum parameter required to run the tool is either a source IP address or a destination IP address.

Command parameter	Description	Format
-s	Source IP address	IPv4 or IPv6 address
-d	Destination IP address	IPv4 or IPv6 address
-p	Port	Text value or integer
-P	Protocol	Text value or integer



Note: For a cluster where both firewalls are passing traffic, the same command must be run on each node.

- 4) Press **Ctrl+C** to stop the additional policy audit.

Result

To run the tool again, with different parameters, first disable the original command or restart the command line session.



Note: The `aconn` tool switches a setting in `acd` and the kernel. The setting is returned to default on a normal exit. If `aconn` is stopped abnormally, the setting might not return to default. You can forcibly disable it with `aconn -D`.

Related concepts

[Transferring audit records](#) on page 307

Related tasks

[Filter audit data](#) on page 296

Troubleshooting access control rules

These sections provide information on troubleshooting basic access control rule problems.



Note: The `cf_policy` man page also contains useful information.

Related concepts

[Allowing and denying audit events](#) on page 666

[Troubleshooting applications](#) on page 669

Related tasks

[Checking failed connection requests](#) on page 667

Allowing and denying audit events

Another troubleshooting tool is `acat_acls`. This real time monitoring tool enables you to display allow and deny audit events as they occur on the firewall.

Use the tool to determine if your access control rules are properly configured or simply view how your rules are being used on a live system.

Examples:

- If you are not certain whether your Telnet rule is properly configured, you can start the monitoring tool, attempt your Telnet connection and see (in real time) whether the connection is allowed or denied.
- If you want to see which rules are currently the most heavily used, start the monitoring tool and watch as the current audit events scroll by within a command window.

The remainder of this section provides information on using the monitoring tool. Information can also be found by typing `man acat_acls` at a firewall command prompt.

Start `acat_acls`

You can use the rule monitoring tool to view allow or deny audit events.

To start the rule monitoring tool, enter the following command at a firewall command prompt:

```
acat_acls -a -d
```

where:

- `-a` = display allow audit events
- `-d` = display deny audit events

If you want to view only allow audit events or only deny audit events, simply omit the undesired option (`-a` or `-d`).

Viewing the output

Each audit event is displayed on a single 80-character line. The source zone and the destination zone fields display the zone index number, not the zone name.

The following example shows both an allow audit event and a deny audit event:

Table 118: Sample audit events

Action	Time	Source zone	Source IP	Dest. zone	Dest. IP	Service
D (deny)	02:41:04	2	192.168.179.76	1	192.168.180.87	ping
A (allow)	02:42:32	2	192.168.179.76	1	192.168.180.87	telnet

Adjust the output

If the output from the monitoring tool is scrolling by too quickly, you can temporarily halt and resume the output.

Steps

- 1) Temporarily halt the output by pressing the following key combination: `Ctrl+S`.
- 2) To resume output, press the following key combination: `Ctrl+Q`
- 3) [Optional] You can also add `|more` or `|less` to a command to control how much output to view at a glance, or redirect the output to a file to view at another time.

Stop the rule monitoring tool

To stop the rule monitoring tool, press the following key combination:

`Ctrl+C`

Checking failed connection requests

If the firewall rejects a connection request that you think should have succeeded, you can take steps to determine why the connection was rejected.

Use the following steps to locate and correct access control rule configuration errors. They will also help you gain a better understanding of how your rules work.

Steps

- 1) Verify that the rule is configured correctly: Select **Policy > Access Control Rules**.

Verify that the rule in question specifies the correct source and destination zones and endpoints. Check all attributes closely, particularly port settings, application defense settings, and assigned authentication method.

- 2) Verify the position of the rules within the **Active Rules** window: Select **Policy > Access Control Rules**., and then click **Active Rules**.

The order of the rules in the **Active Rules** window is important. The attributes of a connection request might sometimes match multiple rules. If the traffic is inadvertently matching a similar rule, move the correct rule before the incorrect rule or adjust some of the properties on the incorrect rule.

- 3) Check the audit log information.

If the connection still fails, scan the audit log to determine which rule denied the connection. See the *Auditing* section for details on viewing audit. The text below displays a common scenario for a connection that failed to match a rule:

```
2012-08-08 10:24:00 -0500 f_http_proxy a_aclquery t_attack p_major
pid: 8333 logid: 0 cmd: 'http' hostname: fw.example.net
category: policy_violation event: ACL deny attackip: 172.22.0.2
attackzone: external application: all srcip: 172.22.0.2 srcport: 24244
srczone: external protocol: 6 dstip: 10.1.1.3 dstport: 80
dstzone: external rule_name: Deny All cache_hit: 0 ssl_name: Exempt All
reason: Traffic denied by policy.
```

- 4) For traffic handled by a proxy, turn on verbose auditing of rule (ACL) checks.

To determine why no proxy rule matched the connection request, type the following command to turn on verbose auditing of rule checks:

```
cf acl set loglevel=4
```

This increases the level of rule audits from the default level 2 (fatal and major errors) to level 4 (fatal, acl allows, and major errors). When the next connection attempt is rejected, the service will generate a more verbose audit message:

```
2012-08-08 10:26:00 -0500 f_http_proxy a_aclquery t_info p_trivial
pid: 8333 logid: 0 cmd: 'http' hostname: fw.example.net
srcip: 172.22.0.2 srcport: 24244 srczone: external protocol: 6
dstip: 10.1.1.3 dstport: 80 dstzone: external
information: Matched SSL rule 'Exempt All'
Skipped matching rule '3': dest IP addr 10.1.1.3 did not match (('ipaddr', 167837957L),).
Matched acl matching rule 10
```

- 5) Run the command `cf policy showtable` to determine the name of the skipped rule.

```
Rule Info ID 3
  Rule Name Inbound HTTP Redirect
  audit=STANDARD
  IPS Not Enabled
  Application Defense Group=minimal proxy
  Auth Groups=None
```

- 6) Compare the skipped rule in the **Access Control Rule** window to the audit. In this example, the incorrect IP address was specified for the destination endpoint in the rule.

- 7) When you are done troubleshooting, type the following command to lower the level of rule audits back to the default:

```
cf acl set loglevel=2
```



Note: If you do not set the log level back to 2, you might run out of disk space.

Result

The traffic should now match the correct rule.

Troubleshooting applications

If your traffic does not match the application you expect, use the firewall audit and **Interactions** tab to see how traffic is behaving.

Using the firewall audit to troubleshoot applications is similar to troubleshooting other aspects of access control rules. Allowed and denied audit entries display the name of the application the connection matched and the rule name that allowed or denied the traffic.

For example, assume your policy is configured to allow web traffic but deny the Facebook application.

This audit entry shows allowed web traffic:

```
2012-07-26 08:12:37 -0500 f_http_proxy a_libproxycommon t_nettraffic p_major
pid: 2783 logid: 0 cmd: 'http' hostname: fw.example.net event: session end
application: SSL/TLS (HTTPS) app_risk: low app_categories: tunnels
netsessid: 80bcf50114243 srcip: 192.168.0.125 srcport: 3042 srczone: internal
protocol: 6 dstip: 10.1.0.146 dstport: 443 dstzone: external
bytes_written_to_client: 3387 bytes_written_to_server: 1286
rule_name: Allow_web cache_hit: 0 start_time: 2012-07-26 08:12:35 -0500
```

This audit entry shows denied traffic for the Facebook application:

```
2012-07-26 08:07:56 -0500 f_kernel_ipfilter a_general_area t_nettraffic p_major
hostname: fw.example.net event: session flush application: Facebook app_risk: high
app_categories: social-networking netsessid: b1d065011412c
srcip: 192.168.0.125 srcport: 2858 srczone: internal protocol: 6
dstip: 172.16.2.3 dstport: 80 dstzone: external bytes_written_to_client: 0
bytes_written_to_server: 0 rule_name: Deny_Facebook cache_hit: 0
start_time: 2012-07-26 08:07:56 -0500
```

In both of these entries, `bytes_written_to_client` and `bytes_written_to_server` are present. The allowed audit entry shows the connection has passed data. In the denied entry, no data has passed.

If traffic is not behaving as expected, you can compare this information to your access control rule list. In some cases, you might have several allow and deny rules that use the same application. If traffic matches one of these rules, but not the rule you expect, use the **Interactions** tab to see how these rules interact.

To access the **Interactions** tab:

- 1) Select **Policy > Access Control Rules**.
- 2) Open the access control rule you expected traffic to match.
- 3) Click the **Interactions** tab.

For information on checking whether a rule is handled by a proxy or packet filter, see Knowledge Base article [9317](#).

Related tasks[Examine how access control rules overlap on page 204](#)

Viewing the audit for SSL rules

To determine whether SSL decryption is working properly, view the audit.

Nettraffic audits

If SSL decryption is working properly, the **nettraffic** audits contain an additional field specifying the SSL rule that triggered for the session.

```
2010-04-26 16:29:57 -0500 f_http_proxy a_libproxycmon t_nettraffic p_major
pid: 6174 logid: 0 cmd: 'http' hostname: spades.g.com event: session end
app_risk: low app_categories: infrastructure netsessid: 1fd04bd605d5
srcip: 10.69.104.140 srcport: 1165 srczone: internal protocol: 6 dst_geo: US
dstip: 206.169.246.160 dstport: 443 dstzone: external
bytes_written_to_client: 1666 bytes_written_to_server: 0
rule_name: allow_outbound_http cache_hit: 0 ssl_name:inspect_outbound_ssl
start_time: 2010-04-26 16:29:57 -0500 application: http
```

This applies to both inbound and outbound traffic.

[Conditional: outbound traffic only] On an SSL-enabled webpage, a user can view the certificate details and verify the certificate issuer. If the firewall SSL Content Inspection functionality is in use, the certificate issuer is a firewall-managed entity.

Display notification

The **Display notification to web browser** configurable is enabled by default.

When enabled, the audit stream periodically contains an entry similar to the following:

```
2010-04-26 16:36:15 -0500 f_http_proxy a_proxy t_info p_minor
pid: 6174 logid: 0 cmd: 'http' hostname: spades.g.com
event: SSL MITM notification netsessid: 5b1c84bd6074f srcip: 10.69.104.140
srcport: 1240 srczone: internal dst_local_port: 443 protocol: 6
src_local_port: 0 dst_geo: US dstip: 151.151.13.133 dstport: 443
dstzone: external attackip: 10.69.104.140 attackzone: internal
rule_name: allow_outbound_http_name: inspect_outbound_SSL
reason: Displayed SSL decryption and inspection notification.
```

If the display notification is enabled, a user periodically sees a webpage notification in their browser.

If the webpage notification does not appear for a Decrypt/Re-encrypt rule, make sure the SSL rule properties and the settings for any access control rules that match the connection are set correctly. SSL decryption notification

window settings are not enforced if an SSL connection matches an access control rule that uses an Application Defense group configured with the HTTP Application Defense set to **<None>** (for example, the connection settings Application Defense group that is initially set as the **<Default Group>** for use in rules).

To troubleshoot display notification, perform these two tasks:

Verify SSL rule properties

You can verify SSL rule properties from the **SSL Rule Properties** window.

Steps

- 1) Select **Policy > SSL Rules**.
- 2) Select the rule, then click **Modify**. The **SSL Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) [Conditional; outbound connections only] On the **SSL decryption settings (client to firewall)** tab, make sure the **Display notification to web browser** checkbox is selected.
- 4) Click **OK** if you have made changes; otherwise click **Cancel**.

Verify access control rule properties

You can verify access control rule properties from the **Rule Properties** window.

Steps

- 1) Select **Policy > Access Control Rules**.
- 2) Select the rule, then click **Modify**. The **Rule Properties** window appears.



Tip: For option descriptions, click **Help**.

- 3) Expand the **Advanced options**.
- 4) In the **Application Defense** drop-down list, check to see if **<Default group>** or **connection settings** is selected.
 - If **<Default group>** or **connection settings** is selected, do one of the following:
 - From the drop-down list, select an **Application Defense** group other than **<Default group>** or **connection settings**, then click **OK**.
 - Change the **<Default group>**:
 - a) Click **Cancel**. When prompted to save your changes, click **No**.
 - b) Select **Policy > Application Defenses > Groups**.
 - c) Select a group other than **connection settings**.
 - d) In the lower pane, make sure the HTTP Application Defense is set to an option other than **<None>**.

e) In the upper pane, click **Set Default**.

f) Save your changes.

If a different Application Defense group is selected, do one of the following:

- From the drop-down list, select an Application Defense group other than **<Default group>** or **connection settings**, then click **OK**.
- Edit the Application Defense group:
 - 1) Click **Cancel**. When prompted to save your changes, click **No**.
 - 2) Select **Policy > Application Defenses > Groups**.
 - 3) Select the Application Defense group.
 - 4) In the lower pane, make sure the HTTP Application Defense is set to an option other than **<None>**.
 - 5) Save your changes.

Determine functioning of HA

This section provides information to determine whether High Availability is functioning properly.

Related concepts

[Viewing status information](#) on page 674

Related reference

[Viewing cluster information](#) on page 673

Viewing cluster information

The `cf cluster status` command gives an overview of the whole cluster, as shown in the following example.

```
HA Cluster Status Information
=====

Primary Host:          fw11v190.example.net
Primary IP Address:    192.168.10.11
Cluster Zone:         heartbeat
Cluster Cert:         Default_Enterprise_Certificate
Cluster CA:           Default_Enterprise_CA

Member Name           State           IP Address
-----
fw11v190.example.net registered      192.168.10.11
fw12v190.example.net registered      192.168.10.12

Policy and Peer Connection Status
=====

fw11v190.example.net (primary)
-----
Connection State : Localhost
Policy Version   : 16-1288461243.12-1288549959
FW Version       : 8.1.0
Status           : Up to date - Current

fw12v190.example.net (peer)
-----
Connection State : Currently Connected
Last Dispatch    : 2010-10-31 13:33:24.396218
Policy Version   : 16-1288461243.12-1288549959
FW Version       : 8.1.0
Status           : Ready
```

Viewing status information

The `cf cluster failover_status` command gives you information on whether or not HA is active, what state the system is in (primary or secondary/standby), and useful statistical information.

Viewing status for a primary

The following example shows sample results for a primary in a load sharing HA configuration.

```

This system is operating in load sharing mode as primary.

This system is node 0.

The secondary is node 1 (192.168.10.12).

Zone 3 is the heartbeat zone

The following cluster addresses are assigned:
heartbeat_network 192.168.10.13
internal_network  10.65.248.13
external_network  10.65.249.13
                 HAtest 1.1.1.5

Failover interface status:
internal_network up
external_network up
                 HAtest up

IP Filter tracking state as load sharing peer

Active firewall list:
node address
  1 192.168.10.12      (secondary)

A backup heartbeat interface is not configured

Statistics for failover

Failover running since Fri Oct  8 11:00:38 2010

Primary since Fri Oct  8 11:04:18 2010

Failover allowing 3 seconds for interface swap (default)

Number of advertisements sent                = 2086390
Number of received advertisements           = 2086307
Number of rcvd advertisements since primary chgd = 2086243
Number of times this system has become primary = 2
Number of release messages received         = 1
Number of release messages sent              = 0
Number of failed takeover attempts          = 0
Number of possible duplicate primary messages = 0
Number of heartbeat ack messages received   = 2086246
Number of heartbeat ack messages sent       = 64
Number of messages received with errors     = 0
Number of same priority advertisements rcvd  = 64

```

Viewing status for a secondary

The following example shows sample results for a secondary that is configured for load sharing HA.

```
This system is operating in load sharing mode as secondary.

This system is node 1.The primary is node 0 (192.168.10.11).

Zone 3 is the heartbeat zone

The following cluster addresses are assigned:

    internal_network  10.65.248.13
    external_network  10.65.249.13
                   HAtest  1.1.1.5

Failover interface status:
    internal_network  up
    external_network  up
                   HAtest  up

IP Filter tracking state as load sharing peer
Active firewall list:
    node  address
      0  192.168.10.11      (primary)

A backup heartbeat interface is not configured

Statistics for failover

Failover running since Fri Oct  8 11:04:15 2010

Failover allowing 3 seconds for interface swap (default)

Number of advertisements sent                = 0
Number of received advertisements           = 2086642
Number of rcvd advertisements since primary chgd = 2086642
Number of times this system has become primary = 0
Number of release messages received         = 0
Number of release messages sent             = 0
Number of failed takeover attempts         = 0
Number of possible duplicate primary messages = 0
Number of heartbeat ack messages received   = 0
Number of heartbeat ack messages sent       = 2086642
Number of messages received with errors     = 0
Number of same priority advertisements rcvd = 2086642
```

Troubleshoot logon issues

This section provides troubleshooting information for the following.

Change authentication for emergency maintenance mode

Change authentication for entering the emergency maintenance mode.

Steps

- 1) Log on to the Admin Console, and select **Maintenance > File Editor**.
- 2) Click **Start File Editor**.



Tip: For option descriptions, click **Help**.

- 3) Select **File > Open**.
- 4) In the **Source** field, select **Firewall File**.
- 5) In the **File** field, type `/etc/ttys` and click **OK**.
- 6) Edit the following line:

```
console none unknown off secure
```

- To require authentication, change the value to `insecure`.
 - To disable authentication, change the value to `secure`.
- 7) Save your changes and close the file editor.

Result

The authentication requirements are now changed.

Change password (forgot)

If you forget your administrator password, you can boot the firewall into emergency maintenance mode (EMM) and reset your password.



Note: By default, the EMM does not require authentication. However, if you configured your system to require authentication for that mode, you will need to temporarily disable EMM authentication before you can enter the mode and change your password.

You must be at the local console to run this procedure.

To change your administrator account password:

Steps

- 1) Restart the system.
- 2) At the Sidewinder boot menu, select **Boot in Emergency Maintenance Mode**.
- 3) Press **Enter** when asked when asked what shell path to use. The system prompt appears.
- 4) Enter the following command to change your password:

```
cf adminuser modify user=name password=newpassword
```
- 5) Restart to the Operational kernel by entering the following command:

```
shutdown -r now
```

Result

You can now log on to the firewall using your new password.

Related tasks

[Change authentication for emergency maintenance mode](#) on page 676

Clear authentication failure lockout

There are two ways to clear an authentication failure lockout.

If you have enabled the authentication failure lockout option and are locked out of your system, have another administrator log on using the Admin Console and clear the lock (see *Authenticator configuration*).

However, if you do not have another administrator who can clear your lock for you, you can still manually clear your lock by successfully logging on at the firewall's local console. When you successfully log on, the lock automatically clears and you can now log on to the Admin Console as usual.

Related concepts

[Authenticator configuration](#) on page 100

Restore firewall access

If an administrator accidentally alters the rule set in a way that prevents an administrator from logging into the firewall (for example, moving the Deny All rule to the first position or deleting certain access rules), use this procedure to restore access.

To regain access to both the local console and the Admin Console:

Steps

- 1) At the local console, restart the firewall.

- 2) At the Sidewinder boot menu, select **Boot in Emergency Maintenance Mode**. A prompt appears stating:
Enter full pathname of shell or RETURN for /bin/sh:
- 3) Press **Enter**. A system prompt appears.
- 4) Restore console access by entering the following:
`cf policy restore_console_access`
This command recreates the default local console and the Admin Console rules. The rules are added to the beginning of the rule set.
- 5) Restart to the Operational kernel by entering the following:
`shutdown -r now`

Result

You can now log on at the local console or with an Admin Console session initiated on the firewall's internal zone.

Check network status

You have these options for checking the firewall network status and basic DNS information.

Related concepts

[Checking the network status using the Admin Console](#) on page 678

[Checking the network status using the command line](#) on page 681

Checking the network status using the Admin Console

From the Admin Console toolbar, click **Tools** to access the following windows for use in gathering network information for troubleshooting purposes.

Use the ARP Table window

Use the **ARP Table** window to view the association between each MAC address on the firewall and its corresponding IP address, as well as the NIC used to reach the IP address.

You can perform the following actions:

- To view an updated table, click **Refresh**.
- To delete an entry in the table, select the appropriate entry and click **Delete**. You can select multiple entries to delete. You can delete all entries by clicking **Delete All**.

To show the host domain name as well as the IP address, clear the **Suppress name resolution** check box and click **Refresh**.

Use the DNS Lookup window

Use the **DNS Lookup** window to find the IP address for a host name.

Steps

- 1) Enter a host name in the **Hostname** field.



Tip: For option descriptions, click **Help**.

- 2) Click **Lookup**. IP addresses associated with the host name appear in the lower pane.

Use the Get Route window

Use the **Get Route** window to find the first gateway in the route from the firewall to a stated destination.

Steps

- 1) In the **IP address or hostname** field, enter a destination. To find the IP address for a host name, type the name and click **DNS Lookup**.



Tip: For option descriptions, click **Help**.

- 2) Click **Get Route**. The route information appears in the lower field.

- **route to** is the destination
- **gateway** is the first gateway in the route to the destination
- **interface**, **if address**, and **zone** belong to the firewall's interface



Note: To show **gateway** and **if address** as domain names, clear the **Suppress name resolution** check box.

Use the Ping Test window

Use the **Ping Test** window to test interface connectivity.

Steps

- 1) In the **IP address to ping** field, enter an IP address or fully qualified domain name that the ping will be sent to. To find the IP address for a host name, type the name and click **DNS Lookup**.



Tip: For option descriptions, click **Help**.

- 2) [Optional] In the **Commandline flags** field, enter parameters for the ping test. You can enter alphanumeric characters, dashes (-), and underscores (_).
- 3) Click **Start Ping**. The button changes to **Stop Ping** and the ping results appear in the window.
- 4) Click **Stop Ping** to stop the test.

- 5) Click **Close**.

Use the TCP Dump window

Use the **TCP Dump** window to manage tcpdump parameters and to start the tcpdump process.

You can perform the following actions.

- Create, modify, or delete tcpdump.
 - Click **New** and enter interface, output, and filtering information in the **TCP Dump Parameters** pop-up window. The entry appears in the table on the **TCP Dump** window.
 - Select a table entry and click **Modify** to make changes to the parameters.
 - Select a table entry and click **Delete** to remove it from the table.
- Enable or disable an entry by selecting or clearing the check box in the **Enabled** column. Tcpdumps are performed only for enabled entries.
- Save a tcpdump entry by clicking **Save**. The entry will remain in the table for later uses.
- Start the tcpdump by clicking **Start TCP dumps**. The **Running TCP dump** window appears and the tcpdump begins for all enabled entries.

Use the Running TCP dump window

You can check network status using the Admin Console and the **Running TCP dump** window.

Use the **Running TCP dump** window to:

- See the progress of a tcpdump
- Stop the tcpdump
- Save and view the dump files
- The table shows the tcpdump parameters and file size for this occurrence.
- To stop the tcpdump process, click **Stop TCP dumps**.
- To save the dump files, click **Save** and then use the pop-up window to navigate to the desired location. A pop-up window appears for each file. When all files are saved, the **Running TCP dump** window closes.
- To view the dump files, click **Launch pcap viewer**.
 - The Admin Console and firewall do not have a viewer. You must install a third-party tool such as Wireshark to view the dump files.
 - When you click **Launch pcap viewer**, you are first prompted to save the files. Use the pop-up window to navigate to the desired location. A pop-up window appears for each file. When all files are saved, your default viewer appears.

Use the TCP Dump Parameters window

Use the **TCP Dump Parameters** window to select an interface and to set other parameters for a tcpdump.

You can make the following entries:

- **Name** — Enter a name to identify this set of tcpdump parameters.
- **Interface** — From the drop-down list, select the interface to capture network traffic for.
- **Enabled** — Select this check box to enable these tcpdump parameters. Tcpdumps are performed only for enabled entries.

- **Promiscuous mode** — Select this check box to capture packets that do not belong to this interface.
- **Bytes to capture** — Select from the drop-down list:
 - **Header bytes only** — captures only packet headers.
 - **Full packet capture** — captures packet headers and data.
- **Limit output** — From the drop-down list, select a size limit for the tcpdump files. If the limit is reached, the data is deleted and the dump starts over.
- **Filtering** — Select a filter option from the **Template** drop-down list.
 - **No filtering** — captures all traffic.
 - **Single host** — captures traffic for a designated host, and all other traffic is discarded. You can enter a host IP address, a port number, or both. To find the IP address for a host name, type the name and click **DNS Lookup**.
 - **Connection** — captures all traffic for two designated hosts. You can enter IP addresses and a port. To find the IP address for a host name, type the name and click **DNS Lookup**.
 - **Custom** — Enter filters that conform to the tcpdump format. See the tcpdump man page on the firewall for more information.

Use the Traceroute window

View the gateways that traffic passes through on a round trip between the firewall and a destination.

Steps

- 1) In the **Traceroute IP address** field, enter the IP address of the destination. To find the IP address for a host name, type the name and click **DNS Lookup**.



Tip: For option descriptions, click **Help**.

- 2) [Optional] In the **Commandline flags** field, add parameters to the trace. See the `traceroute` man page for more information.
- 3) Click **Start Trace**. The gateways and other route information appear in the lower window.

Result

Traceroute finished appears in red when complete. You can click **Stop Trace** to stop the process earlier.

Checking the network status using the command line

You can use the following commands to display information on the status of your network connections, routing tables, and network utilities.

These commands can provide snapshots of different aspects of your system with command line outputs.

Related concepts[netstat](#) on page 682[dig](#) on page 683[ping](#) on page 683[route get](#) on page 683[traceroute](#) on page 684

netstat

Use these commands to view netstat information.

Listens

When you configure a proxy or a server on the firewall, it will post a *listen* on that port.

To view the status of all active listens, enter:

```
netstat -na | grep LISTEN
```

To view the status of all open connections, enter:

```
netstat -na | grep ESTAB
```

To view the status of all connections waiting for a termination request, enter:

```
netstat -na | grep FIN_WAIT_1
```

To view the status of all connections waiting for enough time to pass, ensuring the remote TCP received the acknowledgment of its connection termination request, enter:

```
netstat -na | grep TIME
```

Troubleshooting network interfaces

You can view the status and statistics of network interfaces at the command line.

To view the status of network interfaces on the firewall, enter : `netstat -in`

To view statistics of network interfaces on the firewall, enter : `netstat -s`

Routing tables

You can view the status of the Operational kernel's available routes and their status.

To see the status, enter the following command at a Sidewinder command prompt:

```
netstat -r
```

For the same results without DNS data, enter:

```
netstat -nr
```

dig

You can use the `dig` command to display DNS information.

The `dig` (Domain Information Groper) command gathers information from DNS based on a hostname or an IP address. The command queries servers based on type (NS for name servers, MX for mail servers, etc.) and has many advanced options. This command is more powerful than `nslookup`.

```
dig hostname
```

```
dig -x ipaddress
```

Here is an example of `dig` output:

```
; <<> DiG 9.3.2 <<> mcafee.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15043
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;mcafee.com.          IN      A
;; ANSWER SECTION:
mcafee.com.          86400  IN      A          66.45.10.76
;; AUTHORITY SECTION:
mcafee.com.          3600  IN      NS         stpdc02.scur.com.
;; Query time: 7 msec
;; SERVER: 10.65.240.246#53(10.65.240.246)
;; WHEN: Mon Jan 8 19:06:52 2007
;; MSG SIZE rcvd: 80
```

ping

The `ping` command checks whether an Internet system is running by sending packets that the remote system should echo back.

As output, `ping` lists how much time it took for the message to travel to the other system and back, the total number of packets sent and received, the percent of packets lost, and the average and maximum time it took for a round trip. To view this information, enter:

```
ping ipaddress
```

route get

The `route get` command looks up the route for a destination and displays the route in the window.

To view this information, enter the following command at a Sidewinder command prompt:

```
route get ipaddress
```

The following shows sample output for this command:

```
# route get 10.136.78.11
route to: firewall1.ext.rack20.dfb.test
destination: default
mask: default
gateway: router.ext.rack6.dfb.test
interface: dc0
if address: firewall1.ext.rack6.dfb.test
region: 1 flags: <UP,GATEWAY,DONE,STATIC>
```

recvpipe	sendpipe	ssthresh	rtt,msec	rttvar	hopcount	mtu	expire
0	0	0	0	0	0	1500	0

traceroute

The `traceroute` command provides information on the gateways an IP packet must pass through to get to a destination.

As input, the command needs the host name or IP address of the destination system. It then sends these IP packets from your Sidewinder to that address. As output, it lists the host names and IP addresses of each system the packets were handed off to and how long it took to send each packet back and forth.

To view this information, enter:

```
traceroute ipaddress
```

Related tasks

[Create a rule to allow traceroute through the firewall on page 271](#)

NTP

Use the commands in this section to verify that NTP traffic is passing as expected.

If NTP is experiencing problems, use the following sections to help determine the cause.

Related concepts

[Firewall as NTP client on page 684](#)

[Firewall as NTP server on page 685](#)

[NTP stopped on page 685](#)

Related tasks

[Restart NTP from a command line prompt on page 685](#)

[Synchronize NTP on page 686](#)

[Verify NTP is running and using the correct time on page 686](#)

Firewall as NTP client

Here is an example of the output of the `ntpd` command, where the firewall is configured as an NTP client and the IP address 100.1.1.199 is the IP address of the firewall's interface that is running NTP.

```
fw:Admn {1} % ntpdc -s 100.1.1.199
remote          local      st  poll reach  delay  offset  disp
=====
*ciscot1-mhk.kans 100.1.1.199 2  128  377 0.06488  0.013563 0.00798
.triangle.kansas 100.1.1.199 2  128  377 0.06522  0.013999 0.00902
.ns.nts.umn.edu  100.1.1.199 16 128  377 0.07059  0.002498 0.00983
```

This is a list of the time servers that the firewall is configured to query for time. The stratum field will tell you whether the firewall is able to communicate properly with the time servers. In this case, the first two entries have a stratum of 2, while the third has a stratum of 16. A stratum of 16 always indicates that the firewall is not synchronizing successfully with a time server. In this case, the firewall was able to communicate properly with the first two servers, but not with the third.

Firewall as NTP server

Here is an example of the output of the `ntpd` command when the firewall is configured as an NTP server and the IP address 100.100.2.200 is the IP address of the firewall's interface that is running NTP.

```
Fw2:Admn {1} % ntpdc -s 100.1.2.200
remote    local      st poll reach delay  offset  disp
=====
100.1.2.50 100.1.2.200 3  128  377   0.06488 0.013563 0.00798
```

This is a list of the NTP clients that are configured to get time from the firewall. The stratum field will tell you if the firewall is able to communicate properly with the NTP clients. In this case, the client 100.1.2.50 has a stratum of 3, which means it is communicating properly. A stratum of 16 would indicate that the client was not synchronizing successfully with the firewall.

In most situations, you can look at the stratum to determine whether or not NTP is configured properly and working. There is additional information in the `ntpd` output that might be useful in troubleshooting NTP issues. However, that information is out of the scope of this document.

NTP stopped

NTP is designed to automatically quit whenever the client's time deviates from the server's signal by more than 15 minutes.

When a deviation of this magnitude occurs, NTP writes a message to file `/var/log/messages` before quitting.

To restart NTP, first set the firewall's clock manually and then follow the directions in the next section for restarting NTP.

Related tasks

[Set the date and time](#) on page 584

Restart NTP from a command line prompt

If the NTP process stops, you can restart the NTP process by doing the following.

Steps

- 1) To start the NTP time server, enter the following command:
`cf daemond restart agent=ntp`
- 2) [Optional] Verify the state of the NTP servers by entering the following command:
`cf server status ntp`

Synchronize NTP

If NTP traffic is not passing as expected, you can verify if synchronization is the cause.

Steps

- 1) If you are having synchronization problems, enter the following command:

```
ntpdc
```
- 2) [Optional] Use `man ntpdc` to see detailed information.

Verify NTP is running and using the correct time

You can check to see if NTP is running as expected in several ways.

- Check that the NTP daemon is running on the time server that is serving time to the firewall:

```
ps -df |grep ntpd
```

If `ntpd` is not running, correct this problem before proceeding.

Run the `ntpdate` command to show that the NTP daemon is responding to the request:

```
ntpdate -q -u server_ip
```

where `server_ip` is the IP address of the time server. This command also reports if the queried server time is different from the firewall's system time. To check the time on a firewall-hosted NTP server, use the IP address of the zone where the NTP server is running.



Note: To run the above commands, you need command line access to the NTP server.

- Check the process to see that the firewall NTP server is enabled and running:

```
pss ntpd
```

```
cf server status ntp
```

- If you have NTP properly configured and enabled, you should be able to monitor NTP packets being sent/received on the appropriate firewall interfaces. To do so, enter the following commands:

```
tcpdump -npi if_name udp port 123
```

where `if_name` is the interface and number that you are troubleshooting (for example **em0**, **em1**, etc.)

In the `tcpdump` output, check to make sure that NTP packets are being both sent and received. If traffic is not flowing both ways, verify the routing connectivity between your firewall and the NTP server.

- To check the firewall's exact system time, enter the `date` command and compare it to a known good clock source (for example, <http://www.time.gov>).

Startup

This section contains troubleshooting information for the following issues.

Related concepts

[Connectivity and misconfiguration](#) on page 687

[Licensing](#) on page 688

[Newly installed or re-imaged firewalls](#) on page 690

Related tasks

[Troubleshoot startup network interfaces](#) on page 688

Connectivity and misconfiguration

The following table lists some connectivity and misconfiguration problems and their possible solutions. It also includes DNS and mail configuration troubleshooting guidelines. These problems are most likely to occur immediately after initialization.



Tip: Set up a local console to troubleshoot Sidewinder problems. For information on using a serial terminal connection with the firewall, see Knowledge Base article [8869](#).

Table 119: Connectivity problems and solutions

Problem	Possible cause	Possible solution
Error message: Failed to connect to SSL server	The firewall might not have finished starting up. The network connectivity between your management station and your firewall might have failed. The firewall's IP address is wrong on the firewall or in the Admin Console.	Try connecting again in a few minutes. Check your network connectivity and check the default administration route that you entered in the Quick Start Wizard. Double-check the IP addresses you entered in the Quick Start Wizard.
Error message: Activation key has expired	Firewall license is not currently activated.	License the firewall so it can begin passing and monitoring traffic. See <i>Activate the license</i> for details.
DNS traffic is not passing through firewall	DNS rule is not enabled.	Use the Admin Console to enable the dnsp to all external resolvers rule in the Rules window.
Need to switch from transparent DNS to hosted DNS	Change in security policy	Use the Reconfigure DNS tool in the Admin Console to change your DNS configuration. See the <i>DNS (Domain Name System)</i> chapter for details.

Problem	Possible cause	Possible solution
Mail not passing through the firewall	Mail rules and servers not configured as expected.	Use the Reconfigure Mail tool in the Admin Console to change your mail configuration. See the <i>Email</i> chapter for details.

Related concepts

[Activating the license](#) on page 56

Licensing

If the firewall comes up in failure mode because it did not license during the restart, check the following.

- Try to obtain the license by entering:
`cf license get`
- Verify that there is a default route by entering:
`netstat -nr`
If there is not a default route, add it back with
`cf route add route=default gateway=aaa.bbb.ccc.ddd`
where `aaa.bbb.ccc.ddd` is the next hop router for the default route.
- Verify that DNS is resolving by entering:
`dig www.forcepoint.com`
- Obtain the license by doing one of the following:
 - If DNS is resolving, enter `cf license get`.
 - If DNS is not resolving, you will need to get the license using the activation server's IP address by entering the following on a single line:
`cf license get activation_url=https://161.69.13.69/activation.cfm`
- Restart the firewall again by entering:
`shutdown -r now`

The firewall should now be correctly licensed and fully functional.

Troubleshoot startup network interfaces

If the firewall's initial routing information is incorrect (such as misconfigured IP addresses and netmasks), you must change this information directly on the firewall's local console.

Use the following commands to help you review and edit this information.

These steps assume you have only two interfaces configured, with a cable connecting each interface to its respective network or subnet.

Steps

- 1) From a console attached to the firewall, log on and enter `sr0le` to switch to the Admn domain.

- 2) Enter `cf interface q` to display the interface configuration. Check the following:
 - The IP address (`ipaddr`) and netmask (`mask`) shown for both interfaces (`entrytype=interface`) are appropriate.
 - Both interfaces are enabled (`enabled=yes`).

If any information is incorrect, enter `man cf_interface` for information on correcting it.

- 3) Enter `ifconfig -a` to get the status of the network interfaces. Check the following:
 - Both interfaces' flags include `UP` and `RUNNING`.
 - Both interfaces' speed values (`10baseT`, `100baseTX`, or `1000baseT`) and media type values (most likely `autoselect`) are as expected.
 - Both interfaces show `status: active`. If the `ifconfig` output shows `status: no-carrier`, then no cable is connected to the interface or the device at the other end of the cable is misconfigured or not powered on. Follow standard troubleshooting techniques to resolve the problem.



Note: The external interface on the firewall is automatically configured to discard ping requests.

If any information is incorrect, enter `man ifconfig` (temporary changes) or `man cf_interface` (permanent changes) for information on correcting it.

- 4) For systems configured using DHCP, enter the following command to check routing information:


```
netstat -nr
```

Verify that the routing information is appropriate for this firewall.
- 5) Send a ping from each interface by entering the following command: `ping IPaddr` where `IPaddr` is the address of another host (configured to respond to ICMP ping requests) on the same network segment as the firewall.
 - If both ping commands report ping replies, the firewall is cabled correctly.
 - If only one ping command reports a ping reply, track the fault in the network that is not responding.
 - If neither ping command reports a ping reply, the internal and external cables might have been swapped when inserted into the firewall. Physically swap the cables.



Note: Physical aspects of your cables might require you to swap interface parameters instead of swapping cables. You can swap parameters on the Admin Console at **Network > Interfaces**. Swapping interface parameters can have unexpected results. We recommend that you contact technical support for assistance.

- 6) [Conditional] If you modified interfaces, restart the firewall.

Newly installed or re-imaged firewalls

If you are having difficulties with a new or re-imaged Sidewinder, attach a console to the appliance. The appliance will display messages on the console that can provide information about the system's state.

Table 120: Conditions when you should attach a console

What is happening	How to start troubleshooting
Nothing happens when you turn on a new or newly re-imaged system.	Firewall might be ready for its Quick Start information. Configure the firewall using the Quick Start Wizard or Quick Start Program.
While using the Quick Start Wizard's removable media method, the system does not restart.	There might be non-content errors on the Quick Start Wizard media. Try again with a new Quick Start Wizard USB drive or diskette.
While re-imaging, the system does not restart.	You might need to remove media from the firewall drives. Remove media and restart.
You get an error every time you try to connect with the Admin Console.	This might indicate a network failure. Troubleshoot your network connectivity.

System status

Use the commands in the following sections to display information on the current status of your network connections and view what is happening on the system.

Related concepts

[Administrator activity](#) on page 690

[CPU usage](#) on page 691

[Disk usage](#) on page 691

[Process status](#) on page 691

Administrator activity

You can view which administrators are currently logged onto your Sidewinder.

To view which administrators are currently logged on, enter the following command at a Sidewinder command prompt:

```
who
```

When you use this utility, you can see the administrator's logon name, console name, the date and time of their logon, and their host name if it is not a local host.

```
lloyd          tty??          Feb 23         22:11         (a.example.com)
lloyd          ttyp0          Feb 23         21:34         (10.1.1.1)
```

CPU usage

CPU usage allows you to obtain information on system performance.

To view CPU usage information, enter each of the following commands at a Sidewinder command prompt:

```
vmstat
uptime
top
```

Disk usage

This information is useful to determine which file systems are using the most disk space.

To view statistics about the amount of free disk space on a file system, enter the following command at a Sidewinder command prompt:

```
df
```

Process status

View the status of all process currently running on the firewall.

Enter either of these commands at a Sidewinder command prompt:

```
ps -axd
pss processname
```

This information is useful for tasks such as determining which processes are using excessive CPU time. The `pss` command allows you to look at information about the processes running on the system. This command is a variation on the standard `ps` process status command in that it includes information on the Sidewinder domains. To display process information, enter:

```
ps -d
```

This command lists process information as well as information on the domains in which processes are operating.

In addition to the standard information displayed with the `ps` command, the `-d` switch provides the following additional information:

LABEL	PID	TT	STAT	TIME	COMMAND
secureos/Dmnd	189	con	Ss+	0:01.30	/usr/libexec daemond
secureos/Admn	1360	p	OR+	0:02.05	ps -d

where:

- LABEL — domain name
- PID — process identification number
- TT — terminal line from which the process was initiated
- STAT — current status of the process
- TIME — total amount of CPU time used by the process
- COMMAND — command line used to start the process

Troubleshooting transparent (bridged) mode

For information on troubleshooting transparent mode, see Knowledge Base article [9215](#).

Troubleshooting VPNs

In addition to standard logging, the firewall also performs auditing of certain system events which allows you to generate information on VPN connections.

The table provides useful commands for use in tracking VPN connections in real time mode and checking VPN settings and configuration.

Table 121: Basic VPN troubleshooting commands

Command	Description
<code>tcpdump -npi ext_if port 500 or proto 50 or proto 51</code>	Show IPsec, ESP, and AH traffic arriving at the firewall.
<code>tcpdump -npi if_name udp port 4500</code>	Show NAT-T traffic arriving at the firewall.
<code>cf ipsec q</code>	Review VPN policies.
<code>cf ipsec policydump</code>	Determine if VPN is active. The presence of SPI and transform numbers indicates the secure connection is functioning.
<code>showaudit -vk</code>	<p>Show detailed audit trace information for VPN in real time. To enable a more detailed auditing level, adjust the ISAKMP server's audit level:</p> <ol style="list-style-type: none"> 1) In the Admin Console, select Network > VPN Configuration > ISAKMP Server. 2) Set the audit level to Verbose. 3) Click OK on both windows. 4) Save your changes.

Contacting technical support

If the issue was unable to be resolved, technical support is available.

Go to <https://support.forcepoint.com>. You can find various resources to assist you, including Knowledge Base articles, product documentation, and several ways to contact technical support.

Before contacting technical support, make sure that the following requirements are met and this information is available:

- A valid grant ID
- Sidewinder software at a supported version
- Appliance model and platform
- Hardware serial number
- If applicable, High Availability cluster type
 - Load sharing
 - Peer-to-peer
 - Primary/standby
- Description of the problem

To assist with troubleshooting, have the following available, if possible:

- SSH enabled, for remote access
- Relevant log files
- Error messages
- Any recent configuration or network changes
- Network topology
- Physical access to the firewall
- Any troubleshooting done before contacting technical support

Re-installation and recovery options

Contents

- [Need for re-installation and recovery](#) on page 695
- [Recovery options](#) on page 696
- [Re-installing options](#) on page 700
- [Re-install your firewall from the virtual CD](#) on page 700

If firewall experiences a severe software or hardware problem, solutions range from a rollback to a previous restore point (to resolve short-term problems) to re-installing a full backup onto new hardware.

Need for re-installation and recovery

There are two main solutions for addressing a severe software or hardware problem on the firewall.

- **Recovery options** — Use a recovery option if the firewall experiences a short-term problem. For example, use the rollback feature to recover from an issue caused by a recently installed patch.
- **Re-installation options** — Use a re-install option if the firewall experiences a serious hardware failure or is being repurposed.

The following table lists common problems and their recommended solution.

Table 122: Problems and solutions

Problem	Solution
Patch upgrade failed or caused unexpected behavior	Use the uninstall or rollback option.
Software or configuration disaster	Select the least disruptive option: configuration restore, uninstall or rollback, or re-install.
Repurpose system in some way, such as moving a firewall from one network to another	Re-install and create a new configuration.
Hard disk failure or system replacement	Re-install and restore an existing configuration.

Related concepts

[Recovery options](#) on page 696

[Re-installing options](#) on page 700

Recovery options

Occasionally, you might experience a situation where you need to restore your firewall to a working configuration. Sidewinder has several recovery options to fit different severities and types of situations. Do the following to maximize recovery success:

- Create configuration backups on a regular basis.
- Create disaster recovery backups after installing a new patch.
- When selecting a recovery option, always attempt the least disruptive option first and determine if that solves your problem.

These following sections describe the available recovery options.

Related concepts

[Configuration restore](#) on page 696

[Uninstall](#) on page 696

[Configuration rollback](#) on page 697

[Disaster recovery](#) on page 697

Configuration restore

The policy configuration restore replaces the current firewall policy with a saved configuration file.

Create configuration backups frequently to ensure you have an up-to-date configuration backup from when the policy was known to be configured correctly.

Use this option for the following:

- When misconfiguration or data corruption renders the current policy unacceptable
- To return to a recent configuration after completing a re-install

Before using configuration restore, first try fixing the configuration using these commands:

- `cf policy repair`
- `cf config repair`

Related concepts

[Backing up and restoring the firewall configuration](#) on page 606

Uninstall

The uninstall option removes a patch but maintains the current configuration.

Patches can be uninstalled individually or several at a time. Patches that can be uninstalled are listed with an **Uninstall status** of **Yes** on the **Software Management** window. They are often smaller patches such as vendor patches or hotfixes that do not include features or substantial changes.

Uninstall a patch when it fails to install or introduces behavior that is incompatible with your policy.

To recover from installation failures for patches that don't support this feature, read *Rollback the firewall*. This procedure is an option in the **Maintenance > Software Management** area.

Related tasks

[Manage software packages](#) on page 588

[Rollback the firewall](#) on page 594

Configuration rollback

The rollback option reverts your firewall to the previous restore point, which is a snapshot of the patch level and policy configuration just before the most recent patch was installed.

If multiple patches were installed at the same time, then the restore point is before the earliest patch.

Use this option when a newly installed patch fails to install or introduces unexpected behavior that is incompatible with your policy. With the rollback option, all configuration changes made between when the problematic patch was installed and when the rollback was initiated are lost.

This procedure is an option in the **Maintenance > Software Management** area. See *Rollback the firewall* for information on scheduling and initiating a rollback.

Related tasks

[Rollback the firewall](#) on page 594

Disaster recovery

This option automatically saves the necessary configuration information, patches, and hotfixes to a USB drive.

Use this option when recovering from a failed hard drive or when configuring a replacement firewall. Create backups often to ensure that you can quickly return to the correct patch level and configuration.

Benefits of disaster recovery

The disaster recovery restore option restores your firewall to a previous patch level and configuration by restoring files from a USB drive containing a disaster recovery backup.

This backup includes all installed patches, an initial configuration, and a standard configuration backup file. This option is an efficient way to return your firewall to its previous patch level and a known configuration. If you have a configuration backup that is more recent than your disaster recovery backup, you might want to restore it after the recovery completes.

Use this option to recover after replacing a hard disk or entire system, or if the policy becomes seriously misconfigured or corrupt.

Note the following:

- Disaster recovery backups can be saved only on a USB drive. See *What is required to select a USB drive*.
- Do not alter the disaster recovery backup file.
- The disaster recovery files are intended to be restored on the same hardware that they were created on. If you attempt to restore the backup to different hardware, expect to make significant adjustments.



CAUTION: Failure to follow the above guidelines could corrupt the disaster recovery backup.

Related concepts

[What is required to select a USB drive](#) on page 698

What is required to select a USB drive

Your USB drive must meet several requirements.

- Supported USB drive sizes are 1 GB, 2 GB, 4 GB, and 8 GB. The USB drive must be large enough to hold the configuration and patches. In general, a 1 GB USB drive should be sufficient for most firewalls. Configurations with large home directories might require a larger size.
- Your USB drive must be formatted in MS-DOS.
- The firewall USB port must be enabled in the BIOS settings.

Creating a disaster recovery USB drive

Create a recovery USB drive that includes the configuration and installed patches that were on the firewall when the recovery media was made.

Create the USB drive using the **Create Disaster Recovery Backup** option on the **Configuration Backup** window (**Maintenance > Configuration Backup**).

Related tasks

[Use the Configuration Backup window](#) on page 698

Use the Configuration Backup window

Create a disaster recovery USB drive.

Steps

- 1) Insert a USB drive into one of the firewall USB ports.



CAUTION: This process will overwrite previous disaster recovery backups contained on this USB drive.

- 2) Select **Maintenance > Configuration Backup**.
- 3) Click **Create Disaster Recovery Backup**. The **Configuration Backup: Disaster Recovery** window appears.



Tip: For option descriptions, click **Help**.

- 4) [Optional] Enter a key to encrypt the disaster recovery backup. Valid values include alphanumeric characters, periods (.), dashes(-), and underscores (_).
 - This key will not be saved. You must remember it. You will not be able to restore the disaster recovery backup without this key.

- You do not have to enter an encryption key. If you click **OK** without entering an encryption key, the backup continues.

Enter the key again to verify.

5) Click **OK**. A warning message appears.

6) Click **Yes** to confirm the backup.

A progress bar appears while the files are backed up to the USB drive.



Note: Do not remove the USB drive from the firewall until the “Disaster recovery successful” message appears.

When the backup is complete, a “successful” message appears.

7) Click **OK**.

Result

The disaster recovery USB drive has been created.

Restore the backup

Restore the disaster recovery configuration.

Steps

1) Verify you have the necessary tools:

- Sidewinder Installation CD or USB drive
- USB drive containing the disaster recovery backup

2) Insert the disaster recovery USB drive and the installation media into the firewall.

3) Follow the appropriate re-installation method.

For instructions on re-installing a firewall using the installation media, refer to the *Forcepoint Sidewinder Release Notes*

4) Immediately after the re-install completes, remove the installation media from the firewall.

5) Leave the disaster recovery USB drive in the firewall USB port until the recovery is complete. You can remove the drive after the `Admin` prompt appears, or leave the USB drive in the firewall for future use.

Result

The firewall is now restored to the patch level and configuration saved in that backup.

Re-installing options

Use one of the re-install options when the firewall has experienced a serious hardware failure, such as a failed hard drive, or when the firewall is to be repurposed, such as moving it from one network to another.

- **Re-installing from the virtual CD (VCD)**

This re-install option restores your firewall using the virtual CD(VCD). During the re-install process, you select which patches to install from a list of packages that were available on the firewall before starting the re-install procedure. This option provides flexibility in what version the firewall will be after the recovery. Make sure you know which patches must be installed to match the configuration backup you intend to restore.



Note: Using this option with disaster recovery media is not recommended, as there is a chance that the selected patches will not match the patches in the disaster recovery media.

- **Re-installing your firewall using installation media**

For instructions on re-imaging a firewall using the installation media, refer to the *Forcepoint Sidewinder Release Notes*.

Before re-installing, determine which process best creates the final configuration that meets your needs. See the table for options.

Table 123: Re-install options

Re-install process	Recovery options
Re-install from the virtual CD	<ul style="list-style-type: none"> • Load or create an initial configuration and restore a configuration backup. • Load or create an initial configuration and create a new policy.
Re-install from the installation media	<ul style="list-style-type: none"> • Create a configuration backup. • Download the appropriate Sidewinder. • Install the Management tools and Sidewinder.

Related tasks

[Re-install your firewall from the virtual CD](#) on page 700

Re-install your firewall from the virtual CD

Re-install your Sidewinder from the virtual CD, which contains a copy of all installed patches.

Re-installing from the VCD is appropriate when the firewall needs to be repurposed or needs to recover from a software or configuration disaster, and the hard drive is still functional. This option gives you the opportunity to select which packages to install.

Note the following:

- This method does not require installation media.
- Plan your restore method before you begin. Options include:

- Load or create an initial configuration, and create a new policy.
- Load or create an initial configuration and restore a configuration backup. Know which patches need to be installed to match the configuration backup you intend to restore.
- If you are using a serial terminal for this procedure, use the hot keys to make selections. Using the arrow keys might have unexpected results.

To re-install from the virtual CD:

Steps

- 1) Power on or restart the firewall.

After the standard boot information completes, a menu similar to the following appears:

```
1 Virtual CD
2 Alternate System
3 Operational System

Default: 3
```

- 2) Press **1** to enter the Virtual CD.

- 3) Select a boot option:

- To accept the default installation option, press **Enter**.
- If you intend to use a serial console, type **4** and press **Enter**.



Note: The **Emergency Maintenance Mode** option, the **Boot with ACPI** option, and the **Escape to Loader Prompt** option are generally only to be used on instruction from technical support and are not appropriate for this procedure.

The VCD Main Menu appears, displaying the following options:

```
Select and Install - Select and install MFE Packages
Maintenance Shell - VCD Maintenance Shell Menu
Advanced Menu - Advanced Install Menu
[RTN To select] X Exit Install
```

- 4) Press **S** to select `Select and Install`, and then press **Enter**.

A menu appears listing all available packages.

- 5) [Conditional] If selecting packages:

- Use the hot keys or the up and down arrows to move among the packages. (If using a serial connection, use only the hot keys.)
- Use the space bar to select a package or clear a previous selection.
- Press **O** for **OK** when ready to install the selected packages.
- Press **C** to cancel and return to the previous menu.

- 6) [Conditional] After pressing **O** for **OK**, you are prompted to confirm your selection. Press **Y**.

The packages install. When installation is complete, the VCD Main Menu appears again.

- 7) Press **X** to exit. You are prompted to confirm your decision and reminded to remove all media from the floppy and CD drives.

- 8) Press **Y**. The firewall restarts.

- 9) At the Forcepoint Sidewinder menu, accept the default, which is the Operational System.
- 10) At the boot menu, select a boot method.
- 11) Provide the appropriate initial configuration using one of these methods:
 - Insert a USB drive containing a disaster recovery backup. License information is included in the backup file.
 - Run your chosen Quick Start method. (See the *Sidewinder Setup Guide* for more information.) The firewall tries to send the license activation request to an Internet activation server for one minute. If the activation is not successful in that time, you must activate your firewall using the Admin Console.
- 12) Connect to your firewall using the Admin Console.
- 13) [Conditional] If you need to restore a configuration backup, select **Maintenance > Configuration Backup** and restore your firewall configuration data.

Result

Your firewall is now re-installed.

Related concepts

[Disaster recovery](#) on page 697

[Backing up and restoring the firewall configuration](#) on page 606

Glossary

A	
access control rule	Enforces policy on connections that attempt to pass through or connect to the firewall.
activation key	A string of numbers and characters that allows the operation of the software.
Admin Console	The graphic user interface (GUI) used to configure and manage the firewall.
aggregate	See <i>link aggregation</i> .
application	Identifies the network application associated with a connection.
Application Defense	Used to refine access control rules for specific applications and to configure key services such as anti-virus, anti-spyware, and web services management.
Application Defense group	Used in rules to specify advanced application policy; contains a single profile for each Application Defense to populate the group.
Application Defense profile	Contains all configuration options for an Application Defense.
application discovery	Identifies which applications are in use in a zone.
C	
client	A program or user that requests network service(s) from a server.
CGI (common gateway interface)	Any server-side code that accepts data from forms via HTTP. The forms are generally on webpages and submitted by end users.
D	
daemon	A software routine within UNIX that runs in the background, performing system-wide functions.
domain	(1) Relative to networking, the portion of an Internet address that denotes the name of a computer network. For instance, in the e-mail address <i>jones@example.sales.com</i> , the domain is <i>example.sales.com</i> . (2) Relative to Type Enforcement, an attribute applied to a process running on SecureOS that determines which system operation the process might perform.
DNS (domain name system)	A TCP/IP service that maps domain and host names to IP addresses. A set of connected name servers and resolvers allows users to use a host name rather a 32-bit internet address.
E	
editor	A program that can be used to create or modify text files. See also <i>File Editor</i> .
external DNS	External DNS provides a limited external view of the organizational domain. No internal information is available to the external DNS and only the external DNS can communicate with the outside. Therefore, no internal naming information can be obtained by anyone on the outside. The external DNS cannot query the internal DNS or any other DNS server inside a Sidewinder.
F	
failover	See <i>High Availability</i> .

failure mode	Also known as safe mode, a Sidewinder operating state that allows system administration while not allowing network traffic to pass through. A firewall can enter this mode after such conditions as: (a) a failed license check, (b) a restart during which the system detects a problem with an installed patch, (c) a restart during which the system failed to start a critical service, or (d) the audit partition has overflowed.
File Editor	The program available directly in the Admin Console that can be used to create or modify text files. The File Editor communicates with the Sidewinder using a secured connection.
FreeBSD	The operation system used as a base for developing SecureOS. See also <i>SecureOS</i> .
G	
gateway	A network component used to connect two or more networks that might use dissimilar protocols and data transmission media.
H	
High Availability (HA)	A feature that allows a second Sidewinder to be configured either in a load sharing capacity or in "hot backup" (secondary or standby) mode.
host	Any computer connected to a network, such as a workstation, router, firewall, or server.
I	
ICANN (Internet Corporation for Assigned Names and Numbers)	An organization that oversees IP addresses and domain names on the Internet. The goal of ICANN is to ensure that all public IP addresses are unique and that valid addresses are accessible to all Internet users.
identity validation	Establishes the identity of a user trying to gain access to or through the firewall.
inbound connection	Connection that passes from the Internet zone to the protected zone.
internal DNS	Manages information only available to internal machines. The internal name server cannot receive queries from external hosts since it cannot communicate directly with the external network. Although it is unable to communicate directly with external hosts, it is able to send queries and receive the responses via the external DNS.
Internet	A worldwide system of computer networks. A public, cooperative, and self-sustaining network of networks accessible to hundreds of millions of people worldwide. The Internet is technically distinguished because it uses the TCP/IP set of protocols.
IPv4 address	A 32-bit address assigned to TCP/IP network devices. An IP address is unique to each machine on the Internet.
IPv6	Internet Protocol version 6. A replacement for IPv4, which was released in the early 1980s. IPv6 increases the number of available Internet addresses (from 32 to 128 bits), resolving a problem associated with the growth of the number of computers attached to the Internet.
L	
link aggregation	Used to bundle multiple NICs into a group. Sidewinder offers two types of NIC groups: <ul style="list-style-type: none"> • Aggregate — for increased bandwidth • Redundant — for failover purposes
M	
mail server	A network computer that serves as an intermediate station for electronic mail transfers.

MAT (multiple address translation)	The ability for a single interface to support multiple external IP addresses so that inbound connections can be directed based on IP addresses and application. MAT allows connections to be directed to different destinations for the same application based on the destination IP address.
man page	Short for manual page, refers to the online help that is available within the UNIX operating system. For example, entering man ls at the UNIX prompt displays a description of the UNIX ls command.
MX (mail exchanger) records	DNS entries that define where e-mail addresses within domain names get delivered.
N	
name server	A network computer that maintains a relationship between IP addresses and corresponding domain names.
NAS (network access server)	A system that provides dial-up connectivity to your IP network from a bank of dial-up modems.
NAT (network address translation)	Changing the source address of a packet to a new IP address specified by the administrator.
net mask	The way that computers know which part of a TCP/IP address refers to the network, and which part refers to the host range.
NIC (network interface card)	Hardware, like a computer circuit board, that contains a port or jack that enables a computer to connect to network wiring (for example, ethernet cable, phone line, etc.).
O	
operational kernel	The SecureOS kernel that provides the normal operating state, including Type Enforcement controls. When this kernel is running, the firewall can connect to both the Internet and the internal network, and all configured firewall functions are operational.
outbound connection	Connection that passes from a protected zone to the Internet zone.
P	
ping	A command that sends an ICMP message from one host to another host over a network to test connectivity and packet loss.
port	The number that identifies the destination application process for transmitted data. Port numbers range from 1 to 65535. (For example, Telnet typically uses port 23, DNS uses 53, etc.)
primary name server	The DNS server for a domain where the name information is stored and maintained.
protocol	A set of rules by which one entity communicates with another, especially over a network. This is important when defining rules by which clients and servers talk to each other over a network. Important protocols become published, standardized, and widespread.
proxy	A software agent that acts on behalf of a user requesting a network connection through the firewall. A proxy accepts a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, optionally does additional authentication, and then completes a connection on behalf of the user to a remote destination.
Q	
Quick Start Wizard	A Windows-based program that allows you to create an initial configuration for your Sidewinder.

R	
RAID (redundant array of individual disks)	Information is stored on multiple hard disks to provide redundancy. Using RAID can improve performance and fault-tolerance.
redundant	See <i>link aggregation</i> .
registration	The process of authenticating one Sidewinder system to an HA cluster. This process establishes an encrypted, trusted connection between the two systems.
registration key	Character string used for authentication during the registration process.
router	A network device that forwards data between two or more networks, delivering them to their final destination or to another router.
S	
safe mode	See <i>failure mode</i> .
secondary name server	DNS server that downloads and records a backup copy of domain information from a primary DNS server.
SecureOS	The UNIX-based operating system used in Sidewinder. SecureOS is built upon FreeBSD and includes Type Enforcement security mechanisms.
server	A computer system that provides services (such as FTP) to a network, or a program running on a host that offers a service to other hosts on a network.
service	A description of a network communications protocol.
service group	A collection of network services that are defined on the firewall.
SMTP (Simple Mail Transport Protocol)	The TCP/IP protocol that transfers e-mail as it moves through the system.
SPAN mode	In Switched Port Analyzer (SPAN) mode, the firewall passively listens on the network to analyze traffic.
SSL rule	Determines whether the firewall decrypts SSL connections.
subnet	A network addressing scheme that separates a single network into a number of smaller physical networks to simplify routing.
T	
Telnet	A TCP/IP protocol that directs the exchange of character-oriented data during a client-to-server session.
Type Enforcement	A security technology that protects against intruders by preventing someone from taking over the UNIX operating system within Sidewinder and accessing critical files or doing other damage.
U	
URL (universal resource locator)	Indicates the address of specific documents on the web. Every Internet file has a unique URL indicating the name of the server, the directory, and the specific document.
USB drive	A portable flash memory card that plugs into the computer's USB port.
Z	
zone	A set of one or more interfaces and the group of systems connected to each interface that are to be treated the same from a system security policy point of view.

Index

A

- AAAA record [474](#)
- acat_acls [666](#)
- access control rule groups [207](#), [208](#), [208](#), [209](#)
- access control rules
 - about [68](#)
 - acat_acls [666](#)
 - actions [71](#)
 - allow [68](#)
 - attributes [200](#)
 - audit [73](#)
 - browse pane [202](#)
 - creating and configuring [197](#), [203](#), [207](#)
 - deny and drop [69](#)
 - disabling application capabilities [201](#)
 - elements [69](#), [70](#), [200](#), [200](#), [202](#)
 - failed connection request [666](#)
 - Global Threat Intelligence [130](#)
 - initial (default) [32](#)
 - inspecting HTTPS [264](#)
 - interaction with SSL rules [80](#)
 - IPS [124](#)
 - IPv4 to IPv6 [242](#)
 - managing [197](#), [208](#)
 - modifying template and display settings [211](#)
 - NAT [72](#)
 - ordering [81](#), [82](#), [83](#), [208](#)
 - overriding ports [201](#)
 - redirection [72](#), [227](#)
 - source and destination [78](#)
 - troubleshooting [666](#)
 - types [68](#)
 - viewing [209](#)
 - viewing interactions [204](#)
- Access Table mail file [496](#)
- activation
 - manual [57](#)
 - troubleshooting [687](#)
- Active Directory [100](#), [103](#)
- Active Passport
 - about [95](#), [95](#)
 - configuring [96](#), [97](#), [97](#), [99](#)
 - options [96](#)
 - revoking [98](#)
- add-on modules
 - IPS [117](#)
 - SmartFilter [136](#)
- Admin Console
 - about [53](#)
 - adding and connecting to firewalls [54](#)
 - certificate [54](#)
 - configuring properties [565](#)
 - disconnect [55](#)
 - File Editor [601](#)
 - installation [42](#)
 - logging on [54](#)
 - managing access [565](#), [566](#)
 - toolbar [54](#)
- administration
 - management [563](#)
 - SSH [567](#)
- administrator accounts
 - changing password [577](#)
 - managing [575](#), [577](#), [577](#)
 - monitoring [690](#)
 - read-only [575](#)
- alias
 - email [506](#)
 - IP addresses [378](#), [389](#)
 - root [507](#)
- alternate administrator email [36](#)
- alternate policy [249](#)
- anti-relay controls [492](#)
- Application Defense groups
 - about [180](#)
 - Anti-Virus Scanning [182](#)
 - assigning a default group [190](#)
 - configuring [188](#)
 - connection settings [182](#)
 - default group [181](#)
 - managing [188](#), [189](#), [189](#), [190](#), [191](#)
 - minimal proxy [182](#)
 - predefined [182](#)
 - URL Filtering [182](#)
 - URL Filtering and Anti-Virus Scanning [182](#)
 - viewing usage [190](#)
- Application Defenses
 - about [15](#), [73](#), [179](#)
 - Anti-Virus Scanning [180](#)
 - configuring [191](#), [192](#), [248](#)
 - configuring sendmail properties [195](#)
 - connection processing [181](#)
 - connection settings [180](#)
 - default profiles [180](#)
 - duplicating [192](#)
 - expected connections [183](#), [194](#)
 - Generic [181](#), [182](#), [184](#), [194](#)
 - managing [191](#), [193](#), [193](#), [193](#)
 - minimal proxy [180](#)
 - stateful packet inspection [185](#)
 - types [179](#)
 - URL Filtering [180](#)
 - URL Filtering and Anti-Virus Scanning [180](#)
 - viewing usage [194](#)
 - virus scanning [186](#), [187](#)
- application discovery [260](#), [261](#)
- applications
 - custom [170](#), [224](#), [224](#), [237](#)
 - disabling capabilities [201](#)
 - elements of [166](#)
 - firewall [168](#)
 - managing [173](#)
 - managing groups [175](#)
 - overriding ports [201](#)
 - properties [70](#)
 - signature updates [279](#), [600](#)
 - troubleshooting [669](#)

- types [167](#), [170](#)
- usage [165](#), [261](#)
- A record (address record) [468](#), [472](#)
- ARP
 - gratuitous [643](#)
 - Network Defense [340](#)
 - table [678](#)
- attack audits
 - ICMP [339](#)
 - IP [338](#)
 - IPsec [341](#)
 - IPv6 [342](#)
 - TCP [337](#)
 - UDP [339](#)
- attack protection [15](#)
- audit
 - ascii [294](#)
 - audit.raw [284](#)
 - auditbotd [284](#)
 - auditd [284](#)
 - change tickets [310](#)
 - color schemes [291](#)
 - comparing [294](#)
 - copying entries [307](#)
 - crontab editor [313](#)
 - deleting export entries [312](#), [316](#)
 - display notification [670](#)
 - entries [286](#)
 - exporting [307](#), [308](#), [311](#), [314](#), [315](#), [315](#)
 - file reputation [150](#)
 - how it works [283](#)
 - IP tools [295](#)
 - logcheck [283](#)
 - log file options [311](#)
 - log files [286](#), [287](#), [288](#), [312](#), [313](#)
 - managing log files [309](#)
 - messages [286](#)
 - modifying columns [291](#)
 - nettraffic [670](#)
 - network and system statistics [309](#)
 - options [309](#)
 - output [667](#)
 - overview notebook [294](#)
 - policy tools [296](#)
 - rollaudit [283](#), [314](#)
 - signing log files [312](#)
 - syslog [288](#), [315](#), [315](#)
 - ticket ID [305](#)
 - time span [303](#)
 - tools [289](#)
 - viewing [289](#), [293](#), [294](#)
- audit.raw file [480](#)
- audit filters
 - about [296](#)
 - applying [303](#)
 - attack filters [318](#)
 - building [295](#)
 - common filters [297](#)
 - custom [302](#), [304](#), [305](#)
 - deleting [307](#)
 - expression [292](#)
 - filter builder [305](#)
 - filter shade [292](#)
 - managing [303](#)

- syntax [302](#)
- system filters [324](#)
- types [297](#), [297](#)
- viewing [292](#)
- audit responses
 - alerts [317](#)
 - attack [15](#)
 - creating [321](#), [326](#)
 - deleting [324](#), [327](#)
 - email settings [322](#), [327](#)
 - Global Threat Intelligence [135](#)
 - managing [318](#), [324](#)
 - modifying [321](#), [326](#)
 - network probes [328](#)
 - predefined attack filters [318](#)
 - predefined system filters [324](#)
 - Strikeback [317](#)
- authentication
 - clear locks [676](#)
 - failure lockout [676](#)
 - support [100](#)
 - switching methods [104](#)
 - using in policy [246](#)
 - with VPN [510](#)
- authenticators
 - LDAP [100](#), [103](#)
 - managing [101](#)
 - password [100](#)
 - RADIUS [100](#), [104](#)
 - Windows domain [100](#), [103](#)
- auto-recover on reconnect [653](#)

B

- BGP
 - comparing configurations [442](#)
 - configuring [438](#), [439](#)
 - creating a rule [438](#)
 - IPv4 and IPv6 [438](#)
 - overview [437](#)
 - processing options [440](#)
 - viewing configurations [442](#)
- BIND [476](#)
- blackholed IPs
 - attack responses [321](#)
 - Global Threat Intelligence [135](#)
 - IPS responses [119](#)
 - managing [279](#)
 - sendmail [494](#)
 - with signature-based IPS [115](#)
- Boot with ACPI [700](#)

C

- cabling your hardware [43](#), [688](#)
- Certificate Authority (CA) [629](#)
- certificates
 - about [617](#)
 - ePolicy Orchestrator deployment [152](#)
 - exporting [627](#), [628](#), [628](#)
 - firewall [620](#), [620](#)
 - firewall services [623](#)
 - importing [622](#), [626](#)

- loading 627
- managing 617
- remote 623, 625, 626
- SCEP 154, 621, 625
- server 632
- trust 617
- using in policy 263
- VPN 535
- cf interface 688
- change tickets 310
- chtype command 605
- cluster IP address 377
- CNAME record 472, 474
- command line 49, 567, 688
- commands
 - acat 286
 - dig 683
 - mailq 503
 - monitord 584
 - netstat 682
 - ping 683, 683
 - ps 691
 - route 683, 683
 - showaudit 286, 692
 - tcpdump 686, 692
 - top 691
 - traceroute 684
 - uptime 691
 - vmstat 691
- Common Access Card 100
- Common Vulnerabilities and Exposures (CVE) 123
- configuration backups
 - backing up 606, 606, 607, 608, 609
 - disaster recovery 610
 - lite 310
 - managing 611, 613
 - restoring 606, 611, 611, 611, 612, 612, 696
 - scheduling 615
- configuration repair 696
- console access 573, 574, 574
- content inspection, types of 113
- Control Center
 - rapid deployment 36
 - registering firewalls 599
- CPU, process statistics 691
- CPU, self-diagnostics 584
- CRL 629
- cron 314
- crontab editor 313

D

- dashboard 279, 280
- date and time, setting 584
- decryption 16, 213
- default configuration settings 46
- default policy 32
- default route 34, 414
- deployment
 - Control Center 36
 - options 23
- DHCP interface 375, 382
- DHCP Relay 409, 409, 409, 410, 411

- dig command 683
- disaster recovery 610, 697, 697
- disk space 314, 691
- display notification to web browser 670
- Distinguished Names 618
- DNS
 - AAAA record 474
 - about 13, 459
 - access control rule 460
 - adding records 471, 472, 472
 - allow-query 465, 468
 - allow-transfer 465, 468
 - allow-update 468
 - A record (address record) 468, 472, 474
 - BIND 476
 - CNAME record 472, 474
 - configuring reverse lookup zones 474
 - deleting hosts 475
 - deleting sub-domains 471
 - DNSSEC 480
 - editing configuration files 476
 - enabling and disabling servers 475
 - file types 476
 - firewall hosted 459, 461, 462
 - forwarders 463
 - forward zones 466
 - HINFO 472, 474
 - hosts 472
 - logging 480
 - lookup 679
 - master zone 466
 - master zone attributes 468
 - master zone contents 472
 - MX record 468, 470, 472, 472, 474
 - name servers 461, 461, 465, 470, 471
 - notify 465, 468
 - PTR records 474
 - reconfiguring 477, 477, 478, 479
 - resolver IP addresses 34
 - reverse zones 466
 - serial number 468
 - server configuration 463
 - slave zone 466
 - SOA record 468
 - sub-domain 470
 - transparent 459, 460, 460
 - troubleshooting 687
 - TTL value 468
 - TXT record 468, 472, 474
 - zones 466
- domains
 - network objects 85
 - Type Enforcement 604
- DSCP 407
- dynamic routing
 - protocols 13, 413
 - server processing 419
 - specifying NIC and interface names 419
 - synchronizing files 420
 - troubleshooting 456

E

- email
 - see mail [487](#)
- Emergency Maintenance Mode [596](#), [700](#)
- ePolicy Orchestrator [331](#), [331](#), [332](#), [333](#)
- ePolicy Orchestrator deployment
 - configuring certificates [152](#)
- error messages [687](#)
- Escape to Loader prompt [700](#)
- expected connections [183](#), [194](#)
- extended authentication [544](#)

F

- failed to connect to SSL server [687](#)
- failover
 - see High Availability [639](#)
- features of Sidewinder [11](#)
- File Editor
 - about [601](#)
 - creating backup files [603](#)
 - finding and replacing strings [604](#)
 - opening files [602](#)
 - restoring files [603](#)
 - saving files [602](#)
 - using [602](#)
- files
 - DNS [476](#)
 - editing [601](#)
 - permissions [604](#)
- FIPS 140-2 [616](#)
- firewall certificate
 - creating [621](#)
 - importing [622](#)
 - managing [620](#), [620](#)
- firewall-hosted DNS [461](#)
- Firewall Policy Report [262](#)
- Force NDP reset [656](#)
- forward zones [466](#)

G

- general system information [279](#)
- Geo-Location
 - about [17](#)
 - creating objects [257](#)
 - database updates [279](#), [600](#)
 - network objects [85](#)
 - using in policy [257](#)
- get route [679](#)
- Global Threat Intelligence
 - about [16](#), [16](#), [71](#), [128](#)
 - auditing allowed traffic [134](#)
 - blackholing [136](#)
 - configuring a deny access control rule [131](#)
 - configuring for access control rules [133](#)
 - configuring for sendmail [135](#)
 - global settings [133](#)
 - host reputation classes [130](#)
 - in access control rules [130](#)
 - querying host reputation [134](#)
 - restoring default reputation [135](#)

- spam filtering [490](#)
- using in access control rules [131](#)
- using with sendmail [132](#)
- whitelist [133](#)

H

- HA
 - see High Availability [639](#)
- halt system [596](#)
- hardware acceleration [586](#)
- hardware setup [43](#)
- header stripping [497](#)
- heartbeat
 - verification zone [652](#)
 - zone [639](#), [646](#)
- High Availability
 - adding a reservation [647](#)
 - auto-recover on reconnect [653](#)
 - changing the cluster MAC address [655](#)
 - changing the layer 2 mode [654](#)
 - changing the mode [659](#)
 - cluster addresses [641](#)
 - cluster interface properties [654](#)
 - cluster tree structure [649](#)
 - common parameters [651](#)
 - configuring interface test [655](#)
 - creating a cluster [647](#)
 - failover HA [643](#)
 - Force ARP reset [656](#)
 - Force NDP reset [656](#)
 - heartbeat zone [639](#), [646](#)
 - how it works [639](#)
 - individually managed features [651](#)
 - interface [377](#), [386](#)
 - IPv6 support [641](#)
 - joining a firewall to an existing cluster [648](#)
 - layer 2 modes [642](#)
 - load sharing [642](#), [642](#)
 - load sharing requirements [645](#)
 - managing an HA cluster [651](#)
 - modes [641](#)
 - modifying common parameters [651](#)
 - monitor link status [655](#)
 - multicast [652](#)
 - packet filter stateful session failover [186](#)
 - peer-to-peer [643](#)
 - primary-standby [643](#)
 - re-establishing a failed cluster member [658](#)
 - removing a firewall [660](#), [660](#), [661](#)
 - requirements [645](#)
 - restarting a cluster [658](#)
 - SNMP [357](#)
 - soft shutdown [643](#), [657](#)
 - synchronized features [650](#)
 - troubleshooting [672](#)
 - types of [654](#)
- HINFO [472](#), [474](#)
- host name [279](#)
- host network objects [85](#)
- hybrid mode [30](#)

- I
- ICMP
 - Network Defense 339
 - zone support 370
- ifconfig 688
- in-addr-arpa 466
- inbound redirection 225
- initial configuration 43
- initial policy 32
- installation
 - CD 700
 - management tools 42
 - post-setup tasks 61
 - requirements 41
- integration checklist 37
- interfaces
 - about 373
 - configuring 381
 - creating 381
 - default configuration 25
 - deleting 387
 - deleting addresses 390, 392
 - DHCP 375, 382
 - High Availability 377, 386
 - IP addresses 377
 - managing 380
 - managing IP addresses 388
 - mode 23
 - modifying 387
 - renaming 388
 - standard 23, 374, 381
 - swapping parameters 387
 - testing connectivity 395
 - transparent 375, 384
 - transparent (bridged) 25
 - types 374
 - viewing associated NICs 395
 - viewing status 388, 682
 - VLAN 383
- IP addresses
 - cluster primary 377
 - network objects 85
 - troubleshooting 688
- iPlanet 100, 103
- IP Network Defense 338
- IP range network objects 85
- IPS
 - about 15, 114
 - adding signatures to a group 122
 - adding to access control rules 124
 - class types 119
 - configuring 114
 - enabling and disabling signatures 122
 - filtering available signatures 123
 - global signatures 124
 - managing signatures 123
 - modifying signature groups 121
 - processing flow 115
 - response mappings 118
 - responses 115
 - Signature Browser 124
 - signature file updates 117, 279, 600
 - signature groups 120
 - signatures 114
 - with other attack protection tools 116
- IPsec
 - about 510
 - Network Defense 341
 - troubleshooting 692
- IP tools 295
- IPv4
 - configuring addresses 388
 - create a primary address 389
 - creating alias addresses 389
 - re-ordering addresses 389
- IPv4 and IPv6
 - BGP support 438
 - default network objects 367
 - DNS resolution 463
 - interface support 377
 - IPv4-to-IPv6 translation for HTTP 239
 - support 12, 363, 364
- IPv6
 - allowing 236
 - configuring addresses 390
 - creating addresses 390
 - default route 418
 - firewall-hosted DNS 463
 - Network Defense 342
 - re-ordering addresses 391
- ISAKMP server 533, 557
- K
- keys
 - creating 635
 - exporting 636
 - exporting to another Sidewinder 573
 - exporting to an SSH server 573
 - importing 636
 - SSH 634
 - SSL 634
 - VPN 511
- keyword search 492
- L
- LACP 379
- LDAP 100, 103
- license
 - activation 56
 - activation key 58
 - configuring information 59, 59, 60, 60
 - how to 56, 57, 57
 - importing 59
 - relicense a firewall 57
 - trial 56
 - troubleshooting 688
 - verify 56
- listens 682
- load sharing HA 642
- local console 573, 574, 574
- locked out 677, 677
- logcheck 283
- log files
 - DNS 480

- exporting [312](#), [314](#)
- formats [287](#)
- managing [309](#), [313](#)
- options [311](#)
- rolling [312](#), [314](#)
- signing [312](#)

loglevel [667](#)
logon, troubleshooting [676](#)
loopback address [466](#)
ls command [604](#)

M

M4 config file [503](#), [505](#)
MAC address [678](#)
mail

- advanced configuration [494](#)
- aliases [506](#)
- domains [488](#)
- flushing [504](#)
- mailertables [498](#), [500](#)
- managing messages [506](#)
- queues [488](#), [503](#), [503](#), [503](#)
- reconfiguring [492](#)
- redirecting [506](#)
- rules for transparent [492](#)
- sendmail [488](#)
- transparent [487](#), [487](#)
- viewing email on the firewall [507](#)

mailertable files [500](#)
mailq command [503](#)
management

- options [563](#)
- SSH [567](#)
- tools [42](#)

man pages [688](#)
master zone [466](#)
McAfee AppPrism [14](#)
McAfee EIA

- authentication [156](#)
- configuring [156](#)
- heuristic metadata [150](#)
- integration [147](#)
- metadata [147](#)
- Network Intelligence Manager (nimd) [162](#)

McAfee Logon Collector [106](#), [109](#), [109](#), [110](#)
Messages from Forcepoint [279](#), [600](#)
mode

- hybrid [30](#)

monitord command [584](#)
mta domains [488](#)
multicast

- enabling for PIM-SM [446](#)
- in High Availability [652](#)

MX record [468](#), [470](#), [472](#), [474](#)

N

NAT [72](#)
NAT Traversal (NAT-T) [548](#)
netgroup network object [85](#)
netmap network objectss [85](#)
netstat [688](#)

netstat command [682](#), [682](#)
nettraffic audits [670](#)
Network Defenses

- about [335](#)
- ARP [340](#)
- ICMP [339](#)
- IP [338](#)
- IPsec [341](#)
- IPv6 [342](#)
- restoring defaults [337](#)
- TCP [337](#)
- UDP [339](#)

networking features [11](#)
network objects [85](#), [85](#), [85](#)
network probes [328](#)
NIC

- about [373](#)
- interface relationship [378](#)
- managing [392](#)
- restart [394](#)
- swapping parameters [394](#)
- testing connectivity [395](#)

NIC groups

- aggregate [379](#)
- configuring media capabilities [394](#)
- creating [393](#)
- deleting [393](#)
- LAG [378](#)
- managing [392](#)
- redundant [380](#)
- swapping parameters [394](#)
- viewing members [395](#)

non-transparent

- HTTP, configuring [243](#)
- proxies [183](#)

NTP

- about [578](#), [580](#)
- configuring [581](#), [581](#), [582](#)
- deleting servers [583](#)
- firewall client [578](#), [579](#)
- firewall server [578](#), [579](#)
- modifying server settings [583](#)
- reasons for having stopped [684](#), [685](#)
- references [580](#)
- restarting [685](#), [685](#)
- troubleshooting [684](#)
- version number [578](#)

O

OpenLDAP [100](#), [103](#)
OSPF

- comparing configurations [434](#)
- comparing IPv6 configurations [436](#)
- configuring [431](#), [432](#)
- configuring IPv6 [435](#)
- creating a rule [431](#)
- IPv6 [434](#), [435](#)
- overview [429](#)
- processing [429](#)
- processing options [433](#)
- viewing configurations [434](#)
- viewing IPv6 configurations [436](#)

P

- packages
 - downloading [590](#), [592](#)
 - email notification [592](#)
 - installing [587](#), [589](#), [590](#)
 - loading [587](#), [587](#), [589](#)
 - managing [588](#)
 - scheduling installs and uninstalls [591](#)
 - sorting [589](#)
 - types [586](#)
 - uninstall [591](#)
 - uninstalling [589](#)
 - viewing available [588](#)
- packet filters
 - configuring [184](#)
 - High Availability stateful session failover [186](#)
 - stateful packet inspection [185](#), [186](#)
- partition use [279](#)
- Passive Passport [94](#)
- Passport
 - configuring Active authentication options [98](#)
 - configuring for Internet Explorer [99](#)
 - configuring for Mozilla Firefox [99](#)
 - requiring web login [97](#)
- password
 - authenticator [100](#)
 - Change Password Server rule [105](#)
 - changing [104](#), [105](#), [577](#)
 - forgot [676](#)
 - management [104](#)
- peer-to-peer HA [643](#)
- performance report [691](#)
- PIM-SM
 - configuration file [446](#)
 - configuring [444](#), [449](#)
 - configuring bsr-priority [455](#)
 - configuring IGMP [449](#)
 - configuring interfaces [450](#)
 - configuring rendezvous points [450](#)
 - creating rules [445](#)
 - enabling multicast traffic [446](#)
 - enabling or disabling XORP PIMD [454](#)
 - overview [443](#)
 - restarting XORP PIMD [454](#)
 - viewing configurations [456](#)
- ping [395](#), [679](#), [683](#), [683](#), [688](#)
- plugging in your hardware [43](#)
- policy
 - repair [696](#)
 - scenarios [223](#)
 - troubleshooting [663](#)
- postmaster [488](#)
- post-setup tasks [61](#)
- powering down [596](#)
- primary-standby HA [643](#)
- process statistics [691](#)
- proxies
 - non-transparent [183](#)
 - transparent [183](#)
- proxy agents, multiple instantiation [183](#)
- ps command [691](#)

Q

- Quality of Service
 - about [397](#)
 - applying profiles [406](#)
 - configuring [400](#)
 - configuring queue simulated demands [403](#)
 - creating policy [398](#)
 - managing profiles [401](#), [401](#), [401](#), [402](#), [402](#), [402](#)
 - managing queues [403](#), [404](#), [404](#), [405](#), [405](#)
 - queues [398](#)
 - scenarios [398](#)
 - viewing statistics [406](#)
- Quick Start Program [50](#)
- Quick Start Wizard
 - console [49](#)
 - installation [42](#)
 - response form [38](#)
 - running [45](#), [52](#)
 - serial cable [51](#)

R

- RADIUS [100](#), [104](#)
- rapid deployment [36](#)
- read-only
 - administrator accounts [575](#)
- RealTime Blackhole List [494](#)
- recovery options [696](#), [696](#), [700](#), [700](#)
- redirect access control rule [225](#)
- re-imaging [588](#)
- re-installing
 - from the VCD [700](#)
 - options [700](#), [700](#)
- relicense a firewall [57](#)
- remote administration route [34](#)
- remote certificates [623](#), [625](#), [626](#)
- remote identities [633](#)
- restarting [596](#)
- restore console access [677](#)
- reverse zones [466](#)
- RIP
 - configuring [424](#), [428](#)
 - creating an Unbound Server rule [422](#)
 - creating a rule for a server bound to a zone [423](#)
 - enabling for multiple zones [427](#)
 - enabling on a single zone [426](#)
 - overview [420](#)
 - processing [421](#), [427](#)
 - processing options [425](#)
 - trace and log information [456](#)
- rollaudit [283](#), [312](#)
- rollaudit.conf file [314](#)
- rollback [587](#), [587](#), [594](#)
- routes
 - commands [683](#), [683](#)
 - default [414](#), [415](#)
 - default, IPv6 [418](#)
 - failover [415](#)
 - remote administration [34](#)
 - resetting defaults [418](#)
 - static [414](#), [418](#)
 - viewing status [418](#)

viewing the routing table [682](#)

S

SCEP [621](#), [625](#), [629](#)

scripts [605](#)

secure shell (SSH) [567](#)

sendmail

about [488](#)

advanced configuration [494](#)

allow/deny email on a user basis [496](#)

configuring Application Defense properties [195](#)

configuring size limitations [492](#)

enabling filtering services [490](#)

enabling TLS [495](#)

header stripping [497](#)

M4 config file [503](#)

macros [498](#)

mailertables [498](#)

mail queues [503](#)

masquerading [501](#)

mta domains [488](#)

queue interval [505](#)

RealTime Blackhole list [494](#)

Type Enforcement [488](#)

using with Global Threat Intelligence [132](#)

serial cable [41](#), [43](#), [51](#)

serial connection settings [50](#)

servers

Change Password Server [104](#)

DNS [475](#)

sendmail [488](#)

syslog [288](#)

setup

interfaces [23](#)

planning [21](#)

sftp [567](#)

showaudit [286](#)

shutdown [596](#), [596](#), [597](#)

slave zone [466](#)

SmartFilter

about [17](#), [136](#)

auditing [143](#)

configuring filter policies [141](#), [247](#)

customizing sites [142](#)

database updates [140](#), [279](#), [600](#)

enabling management [139](#)

enabling on an access control rule [144](#)

firewall Admin Console management [137](#), [139](#)

management options [137](#)

SMTP

see mail [487](#)

SNMP

about [345](#)

agent [345](#), [350](#)

agent configuration [351](#), [351](#)

communities [351](#)

configuring rules [357](#)

management station [346](#), [350](#)

MIBs [349](#), [351](#)

pass-through [359](#)

passwords [353](#)

protocols [345](#)

trap destinations [356](#)

traps [329](#), [347](#)

trap version and settings [355](#)

user names [353](#)

v3 users [353](#)

SOA record [468](#)

software

managing packages [588](#)

rollback [697](#)

types of packages [586](#)

uninstall [696](#), [696](#)

updating [588](#)

SPAN mode

about [30](#), [376](#)

creating interfaces [385](#)

creating policy [272](#)

SPI (Security Parameters Index) [546](#)

srole [688](#)

SSH

configuring RSA authentication [570](#)

configuring SSH-2 public key authentication [571](#), [572](#)

connecting to another server from the firewall [569](#)

content inspection [252](#)

keys [634](#)

known host keys [196](#), [252](#), [253](#), [254](#), [255](#), [255](#), [256](#)

managing access [568](#)

SSL rules

about [73](#)

audit [221](#)

configuration process [213](#)

configuring exemptions [250](#)

configuring rule attributes [216](#)

creating [218](#), [267](#)

display notification [670](#)

elements [78](#), [78](#), [79](#), [216](#)

interaction with access control rules [80](#)

keys [634](#)

managing [219](#), [222](#)

modifying [219](#)

nettraffic audits [670](#)

ordering [81](#), [220](#)

outbound [74](#)

source and destination [70](#)

troubleshooting [670](#)

types [74](#)

viewing [221](#)

startup, troubleshooting [687](#)

stateful packet inspection [185](#), [185](#), [186](#)

static route [418](#)

Strikeback [317](#)

sub-domain (DNS) [470](#)

subnet network objects [85](#)

syslog [288](#), [315](#), [315](#), [316](#)

system status [690](#)

T

TCP dump [680](#), [680](#), [686](#)

TCP Network Defense [337](#)

terminal emulator settings [50](#)

ticket ID [305](#)

time, configuring [583](#)

time periods [71](#), [90](#)

- time zone, configuring [583](#)
- tools menu
 - ARP Table [678](#)
 - DNS lookup [679](#)
 - get route [679](#)
 - ping test [679](#)
 - TCP dump [680](#)
 - Traceroute [681](#)
- top command [691](#)
- traceroute
 - from the firewall [681](#), [684](#)
 - through the firewall [271](#)
- transparent
 - DNS [460](#)
 - firewall [25](#)
 - interface [375](#), [384](#)
 - mail [487](#)
 - proxies [183](#)
- transparent (bridged) mode
 - about [25](#)
 - scenarios [25](#)
 - troubleshooting [692](#)
- troubleshooting
 - access control rules [666](#)
 - High Availability [672](#)
 - IPsec [692](#)
 - logon [676](#)
 - network status [678](#)
 - no admin access [677](#)
 - NTP [684](#)
 - SSL rules [670](#)
 - startup [687](#)
 - system status [690](#)
 - transparent (bridged) mode [692](#)
 - VPN [692](#)
- TTL value (DNS) [468](#)
- TXT record [468](#), [472](#), [474](#)
- Type Enforcement
 - file types [604](#)
 - sendmail [488](#)

U

- UDP Network Defense [339](#)
- uninstall [587](#), [587](#)
- UNIX, editing files [601](#)
- updates
 - dashboard [279](#)
 - IPS [117](#)
 - types [600](#)
 - types of packages [586](#)
- UPS (Uninterruptible Power Supply) [598](#), [598](#), [599](#)
- uptime command [691](#)
- URL filtering
 - see SmartFilter [136](#)
- URL translation rules [228](#), [228](#), [229](#)
- usage reports [279](#)
- USB drive [45](#), [45](#), [697](#), [698](#)
- user groups
 - creating external [109](#)
 - creating firewall [108](#)
 - filtering [112](#)
 - managing [110](#), [111](#), [111](#)

- searching for [112](#)
- types [106](#)
- usage [111](#)

- users
 - changing administrator password [577](#)
 - creating [108](#)
 - filtering [112](#)
 - managing [110](#), [111](#), [111](#)
 - searching for [112](#)
 - types [106](#)
 - usage [111](#)

V

- var/log/audit.raw file [480](#)
- var/log/daemon.log file [480](#)
- var/spool/mqueue.X [488](#), [503](#)
- virtual
 - CD [700](#), [700](#), [700](#)
 - zone [518](#), [518](#)
- virus scanning
 - about [17](#), [125](#)
 - Application Defenses [186](#), [491](#)
 - configuring default action [187](#)
 - configuring the number of scanners [126](#)
 - enabling on access control rules [127](#)
 - global properties [125](#)
 - modifying general properties [126](#)
 - rules [187](#)
 - signature file updates [127](#), [279](#), [600](#)
- VLAN interface [375](#), [383](#)
- vmstat command [691](#)
- VPN
 - algorithms [548](#)
 - authentication [510](#), [515](#), [515](#)
 - benefits [509](#)
 - certificates [535](#)
 - client address pools [514](#), [550](#)
 - commands [692](#)
 - configuring [532](#), [535](#), [536](#)
 - encapsulation method [539](#)
 - encryption [510](#)
 - extended authentication (XAUTH) [544](#)
 - IPSec keys [511](#)
 - IPv4 and IPv6 [514](#)
 - ISAKMP server [533](#)
 - keys [546](#)
 - mode [511](#), [514](#)
 - NAT Traversal (NAT-T) [548](#)
 - ordering VPN definitions [518](#)
 - planning [511](#)
 - remote identities [633](#)
 - SPI [546](#)
 - status [538](#)
 - troubleshooting [692](#)
 - virtual zone [518](#)

W

- web filtering
 - see SmartFilter [136](#)
- Windows domain [100](#), [103](#)

Z

zone

- about [12](#), [369](#)
- configuring [370](#), [370](#)
- default [22](#), [369](#)
- deleting [372](#)
- DNS [466](#)
- external [369](#)
- internal [369](#)
- Internet [370](#)
- types [370](#)
- usage [372](#)
- virtual [518](#), [518](#)
- zone groups [371](#), [372](#)

