FORCEPOINT

Sidewinder Control Center

Product Guide

5.3.2P13

Revision A

Published 2018

Table of contents

Maintenance....425

Control Center....441

Preface

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

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	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/Caution:** 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.

What's in this guide

The *Forcepoint Sidewinder Control Center Product Guide* is organized by functional area.

Planning and setup

Set up Control Center for the first time.

Policy

Manage the rules and rule objects for managed firewalls.

Dashboards

Dashboards provide overview information for the firewalls in your network.

Monitoring

Set up firewall auditing and event responses for managed firewalls.

Maintenance

Perform administrative tasks on managed firewalls.

Control Center

Perform administrative tasks on the Control Center Management Server.

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.

CHAPTER 1

Introduction

Contents

Forcepoint Sidewinder Control Center is an enterprise-class management tool for creating and applying security policies across multiple firewalls. Network administrators can remotely manage, maintain, and monitor firewalls for one or more domains.

About Forcepoint Sidewinder Control Center

At minimum, a Control Center deployment consists of a Control Center Client application, a Control Center Management Server, and all managed Sidewinder appliances and Domains.

- **Control Center Client application** — An application that resides on a desktop computer that is running a Windows® operating system. The application provides the user interface to configure, manage, and monitor supported firewalls, and to perform Control Center administrative tasks.
- **Control Center Management Server** — A hardened Linux® platform that provides the firewall management and monitoring capabilities that are required to centrally implement security policy. It manages the framework for secure communication between the server, Client, and supported firewalls. The Management Server requires at least one installation of the Control Center Client. By default, SELinux is enabled to provide secure and controlled access.
- **Managed Sidewinder appliances** —At least one firewall in a heterogeneous network of security devices that exist in a single domain.
- **Domains** — One or more domains that represent a complete, inclusive network security policy.

The Client and tiers of firewalls securely communicate with the Management Server by using SOAP over HTTPS. SSL, using Client Certificates generated by the built-in Certificate Authority, is used to encrypt and authenticate the client/server communication.

You can also implement Management Servers in a High Availability (HA) configuration, in which one Management Server actively manages the registered firewalls, while another Management Server acts as a standby or backup. If the active Management Server fails, the management responsibilities can be switched to the standby or backup Management Server.

The Control Center is used to:

- Define and distribute access control rules to hundreds of firewalls.
- Share configuration data among firewalls.
- Configure Virtual Private Network (VPN) connectivity.
- Implement and selectively activate multiple security policies.
- Manage software releases on all your firewalls.

- Simplify routine administrative tasks.
- Manage ongoing changes to your security policies.

The Control Center supports the following features and functions:

- **Object-based design** — By using an object-based configuration technique, you can define objects once and then reuse them anywhere that the object is needed. Network objects represent one example of this implementation. Network objects include firewalls and device groups, hosts, networks, address ranges, interfaces, and endpoint groups. These objects are used when you define access control rules. Over time, hundreds of rules can be defined by using these objects. If the properties of a network object must be changed, you have to update the object once. The resulting changes will propagate wherever that object is used.
- **Auditing of object management events and archiving of audit tracking data** — You can configure the audit trail settings feature in the Control Center to monitor object changes and purge or archive audit tracking data. The auditing data contains information about the requested operation performed, time, date and user name. This information can be displayed or printed using the **Audit Trail** report. Because the audit tracking table grows without bounds and consumes disk space, you also have the option to periodically remove the data from the database or archive it to another location. This is true for both Control Center audit data and audit data that is currently stored on the Management Server that was retrieved from one or more firewalls.
- **Configuration domains** — You can use configuration domains to partition your managed firewalls into separate collections of objects and configuration data. Each collection is independent of any other collection, and changes to one collection do not affect the others.
- **Rule set queries** — Because firewall configurations often require numerous rules, you can use the Control Center to produce views of rule subsets. This added convenience helps to manage and validate the many rules that are stored in the Control Center database.
- **Firewall configuration retrieval** — After a firewall has been added to the list of managed firewalls, you can use the **Firewall Retrieval Options** window to choose the configuration components to retrieve and store as Control Center objects. You can select all components or limit your selection to specific components. This feature saves time and effort when you are performing the initial setup to manage a firewall.
- **Policy validation and reports** — After making configuration changes, but before applying them, you can determine whether the firewall configurations in the Control Center database are valid. You can view a report that shows the status of the validation process and a report that details the differences between the current and proposed firewall configurations.
- **Configuration status** — After the configuration has been propagated to one or more firewalls, you can view a status page that lists warnings or errors that might have occurred.
- **Certificate Authority (CA) framework** — You can quickly issue certificates for the various architectural components by using a built-in CA framework. A built-in CA saves time when using SSL with client certificates.
- **Simultaneous, multiple users** — You can use the locking mechanism in the Control Center to accommodate simultaneous use of the Control Center Client application by multiple users. Administrators have the option of locking entire object trees or allowing the system to lock individual objects on a first-come, first-served basis. This approach allows single-user environments to function without explicit locking.
- **High Availability (HA) feature** — You can configure redundant Management Servers by using the High Availability Server Configuration (HA) feature. The HA feature uses a multi-server configuration to continue Management Server functions if the active Management Server fails.

About the Client application

The Control Center Client application is an application that provides the user interface for task-grouped operations on the Control Center.

The Control Center Client application has five icons that group functions into similar areas so that you can locate and perform the firewall and Control Center management tasks more easily.

Dashboards icon

The **Dashboards** icon provides a visual way to quickly track the status of the firewalls and the Control Center Management Server.

You can view the following information in the **Dashboards** icon:

- **View the status of the Control Center Management Server** — The **Summary** page provides a visual display of the status of the Control Center Management Server and general information about alerts, resources, Messages from Forcepoint, and recent configuration changes that have been made.
- **Determine firewall status** — The **Firewalls** page provides a comprehensive visual display of the operational status for all the supported firewalls. This page lists firewall-specific status reports based on the audit log data that is sent to the Management Server by each configured firewall.
- **View the status of various licenses for all of the firewalls** — The **Licenses** page consolidates all the license information into one location.

Policy icon

Use the **Policy icon** to define, configure, and maintain multiple firewalls and security policies for a distributed homogeneous or heterogeneous configuration of firewalls.

You can accomplish the following tasks by using the features and functions of the **Policy icon**:

- **Create configurable rule objects for access control rules** — The components that comprise a security policy include a set of configurable objects that defines the characteristics of the building blocks that are used to implement the security policy. Use this object model of defined objects to share characteristics, options, and functions, instead of having to provide raw configuration information for each aspect of an implemented security policy. Use the **Policy icon** to retrieve, create, and manage configurable object characteristics.
- **Manage configurable rule objects** — After rule objects have been defined or retrieved, you can edit, validate, and apply changes to the configured object. You can manage the implemented security policy across all the supported firewalls in your configuration.
- **Create and manage access control rules** — Access control rules provide the network security mechanism that controls the flow of data into and out of the internal network. They specify the network communications protocols that can be used to transfer packets, the hosts and networks to and from which packets can travel, and the time periods during which the rules can be applied. Access control rules are created by the system administrator and should reflect the internal network site's security policy. Depending on the requirements of your configuration, there might be from hundreds to tens of thousands of access control rule to manage. Use the **Access Control Rules** tab to view and manage these rules.
- **Create setting objects for firewalls** — There is a different set of configurable objects that can be used to help define one or more firewalls. These objects are located on the Firewall Settings tab of the **Policy icon**.
- **Manage setting objects for firewalls** — You can manage these firewall setting objects as standalone entities or you can manage them from within the **Firewall** or **Cluster** window. You can also drag existing objects from the **Firewall Settings** tree to the firewall or cluster in the **Policy** tree.
- **Register and manage firewalls** — Firewalls represent the physical devices that are used to implement a security policy for an organization. They are designed to protect organization IT infrastructure by keeping out unauthorized users, code, and applications, both internally and externally. You can retrieve the settings of existing firewalls or you can configure new firewalls in the **Policy** tree.
- **Maintain access control rules and objects** — Several features are available to help you maintain your list of access control rules, rule objects, and firewall objects. You can combine similar objects or delete duplicate access control rules or objects that are not being used anywhere. These wizards and windows are located on the **Policy Cleanup** tab of the **Policy icon**.

- **Create and manage SSL rules** — SSL rules provide the means for you to determine your decryption policy. Specifically, SSL rules determine whether SSL connections are decrypted by the firewall.
- **Create and manage URL translation rules** — URL translation rules let you map inbound HTTP requests to different destinations.
- **Manage attack and system event responses** — Responses let you configure how managed firewalls will react to audit events. Firewall responses can range from sending email alerts to blackholing host IPs.

Monitor icon

The **Monitor icon** aggregates access to firewall audit data and a wide variety of firewall reports in one icon.

The following functions are available in this icon:

- **Manage audit reports** — You can generate user-defined, firewall-specific audit reports based on the audit log data that is sent to the Management Server by each configured firewall.
- **Generate and view firewall-specific reports** — You can generate and display a variety of firewall-specific reports. For those reports that require it, you provide the report-specific parameters or options for the specific report that is being generated through the provided interface.
- **Generate reports for captured packets of data** — You can manage TCP Dump sessions and use packet captures to more closely evaluate attacks and network failures.
- **View the compliance status of your managed firewalls** — You can display all the managed firewalls and status information for all the firewalls in your configuration that are managed by the Control Center.
- **View Secure Alerts for the firewall** — An integrated Secure Alerts Server collects the alerts and activities that are generated by the supported firewalls. This server also normalizes the data and stores it in the Secure Alerts Server database. This data is the source of information that is presented on the **Alerts** page. Use the **Secure Alerts Server Status** page to view the status of the associated server.

Maintenance icon

The **Maintenance icon** contains a tree and tabs that provide the functions to maintain the settings for multiple firewalls and security policies in a distributed homogeneous or heterogeneous configuration.

- **Re-initialize, restart, and provide an orderly shutdown of selected firewalls** — You can perform these and other functions on selected firewalls in the **Device Control** window. You can also terminate active sessions and security associations for user-selected firewalls.
  You can also set the date and time of one or more firewalls.
- **Back up and restore configurations for selected firewalls** — Use the saved configuration files to restore a default firewall configuration, to maintain a version of a working configuration before you make any configuration changes, or to recover from an unexpected loss of firewall configuration data. When you are installing software updates, this feature is a convenience and a precaution.

Use the tabs on the Maintenance icon to perform the following tasks:

- **View the status of a firewall that was enrolled by using the Sign Up Firewall** — View this information on the **Deployment Status** page.
- **Manage updates to your firewalls** — Determine the current version of software that is installed on each firewall; install, uninstall, or roll back an update; schedule an update action for a particular date and time; view the status of an update action; and view the history of previously completed update actions.
- **Store firewall updates** — Download, manage, and store firewall software updates on the Management Server. Use the interface to identify the name of the update, the type of firewall to which the update applies, the release date, and its download status. You can also view an associated readme file.

Control Center icon

The Control Center icon aggregates the Control Center administrative functions into a single icon.

You can accomplish the following tasks by using the features and functions of the Control Center icon:

- **Settings node** — Use the nodes beneath the **Settings** node on the Control Center tree to manage configuration of various settings of the Control Center Management Server.
  - **View and edit network settings** — You can view and edit Control Center settings, such as host name, servers (NTP, DNS, and mail), network interfaces (IP address, net mask, broadcast, and gateway) and static routes on the **Network Settings** window.
  - **View and edit system settings** — You can manage specific Control Center system settings in the **Control Center** icon. These settings include: specifying the default logon disclaimer information that is posted in the logon window for the Client application, the failed logon lockout settings, and the default application time-out period.
  - **Configure alternate authentication** — You can configure the way that Control Center users authenticate with the Management Server. The Control Center supports an internal authentication mechanism, as well as LDAP and RADIUS for off-box authentication.
  - **Set the Management Server date and time** — You can set the Management Server date and time in the **Date and Time** window.
  - **Manage Management Server properties** — You can display and edit Control Center Management Server properties and add new properties.
  - **Export audit log files from the firewall** — Export firewall audit log files that were written to the Control Center Management Server to a remote location.
  - **Export Control Center audit to syslog servers** — Export Control Center audit data to event message collections, which are also known as syslog servers or syslog daemons.
  - **Configure SNMP Agent** — Use options on this window to configure the Control Center SNMP Agent to send information to a network management system.
  - **Configure settings to communicate with the ePolicy Orchestrator server** — You can configure the Control Center Management Server to communicate with a McAfee® ePolicy Orchestrator® (McAfee ePO™) server to share information about host objects, firewalls, and the Control Center Management Server. To use this communication, you must also configure a McAfee ePO user in this window.
  - **Enable FIPS mode** — You can enable FIPS mode for Control Center using options on this window.
- **Maintenance node** — Use the nodes beneath the **Maintenance** node in the **Control Center** tree to manage the backup and restoration of the Control Center configuration and the operational data. A full system backup can be requested and an off-box location can be specified.
- **Manage administrators** — You can create Control Center administrators who can access the Control Center.
- **Manage LDAP user groups** — You can create LDAP user groups on the Control Center that match the LDAP user groups that have been configured on the LDAP server. You can then configure the attributes and privileges of each group.
- **Manage roles** — After a Control Center user (administrator) is specified, he or she is assigned a role that determines the tasks that he or she is allowed to perform. Although a default set of roles has been predefined, you can create additional administrator-defined roles that can be assigned to Control Center users.
- **Manage configuration domains** — You can implement the configuration domains option to segregate configuration data views and management into multiple domains. The operation and configuration data associated with a configuration domain is accessible only when the specific domain is selected during the logon process. All other configuration data is obscured and cannot be acted upon or seen. If configuration domains are activated, configuration domain versions and version management can be accessed from the Control Center icon.
- **View and manage log files** — You can view and manage the settings to display log files from the Control Center Management Server. Additionally, you can view information about the Management Server.

- **Use the Support Tool to assist Technical Support** — Create and save a configuration bundle file to assist technical support with troubleshooting.
- **Configure High Availability (HA) on the Management Server** — You can use these wizards to establish or remove the High Availability (HA) Management Server configuration.

Also available in the Control Center icon are the following features:

- **Configure MLC connection settings** — Displays the **MLC Connection Settings** page, in which you can view McAfee® Logon Collector objects that contain configuration settings to communicate with the McAfee Logon Collector server.
- **View audit data** — Displays the **Audit Trail** page, in which you can list, filter, preview, and print the audit trail data. This page is read-only.
- **View and configure alert processing rules** — Displays the **Alert Processing Rules** page in the work area, in which you can view all the alert processing rules that are currently available.
- **Update the Control Center** — Displays the **Control Center Updates** page, in which you can manage and install Forcepoint Sidewinder Control Center Management Server software updates.
- **View the status of the backup (Management) Server** — If the High Availability (HA) Management Server Configuration option is used, you can view the status condition of the backup Management Servers in the Backup Server Status page.

PART I

Planning and setup

Contents

Install and configure the Control Center Management Server and Client application.

CHAPTER 2

Plan your Control Center installation

Contents

Understand options for deploying your Control Center and managed firewalls. Plan your network configuration and develop an integration schedule.

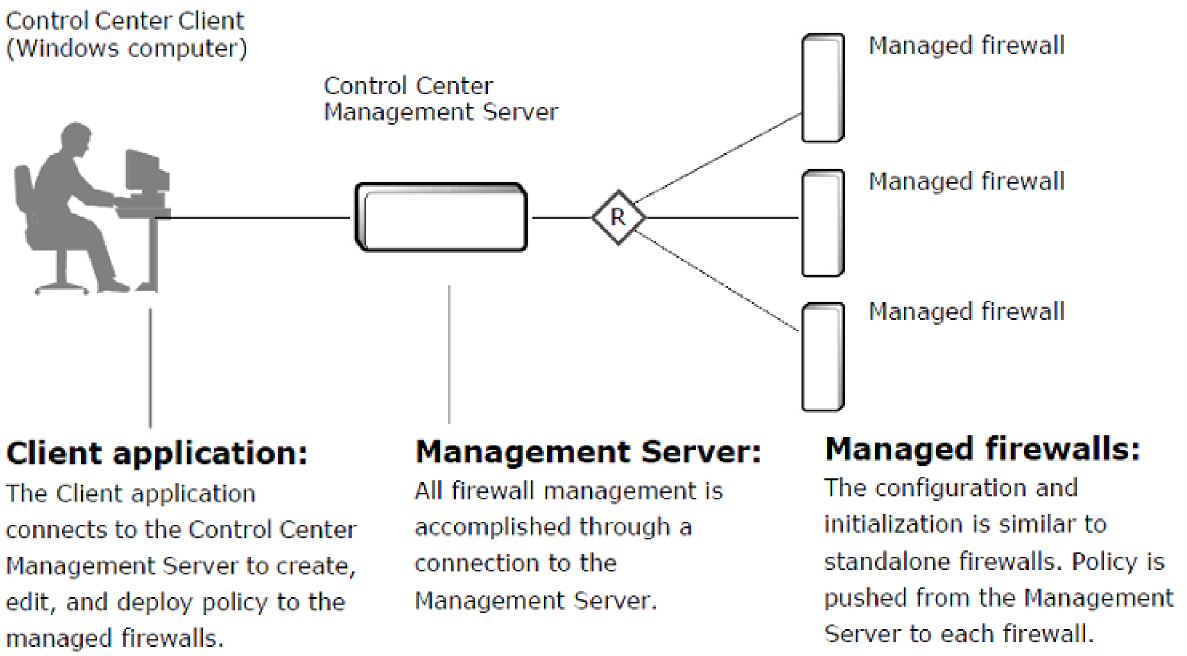
Understanding the Control Center Management Server environment

The Control Center Management Server is an enterprise-class management tool that is used to create and apply security policies across multiple firewalls.

It centrally manages policy, software updates, and reports, and monitors the firewalls in your organization. You can use the Control Center Management Server to manage hundreds of firewalls.

The Control Center uses a Windows workstation that is installed with the Control Center Client application to present a graphical user interface to enterprise administrators. The installation USB drive provides the programs to prepare the initial configuration and to manage your Management Server and its registered firewalls.

Figure 1: Basic Control Center Management Server environment



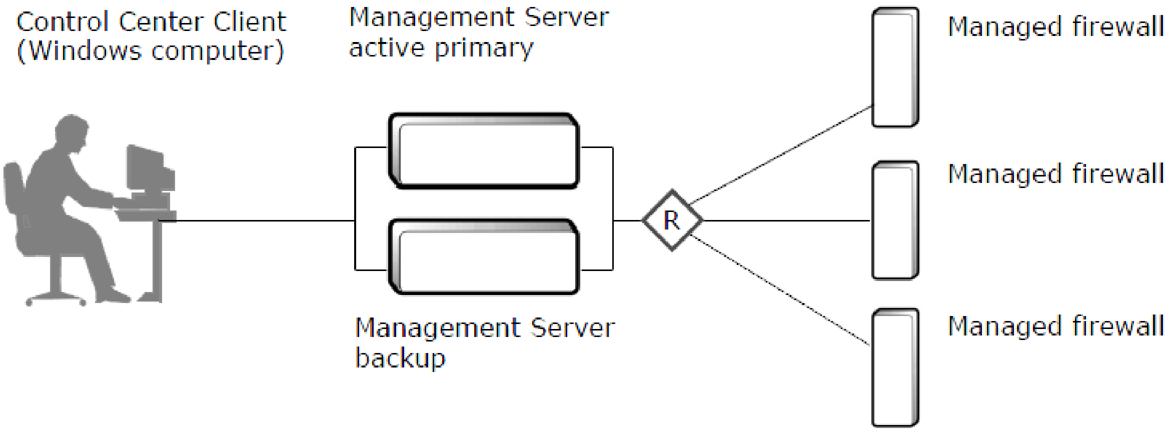
Client application: The Client application connects to the Control Center Management Server to create, edit, and deploy policy to the managed firewalls.

Management Server: All firewall management is accomplished through a connection to the Management Server.

Managed firewalls: The configuration and initialization is similar to standalone firewalls. Policy is pushed from the Management Server to each firewall.

You can also implement Management Servers in a High Availability (HA) Management Server configuration, where one Management Server actively manages the registered firewalls while another Management Server acts as a standby. Use this configuration to manually switch management responsibilities to another Management Server if the active Management Server fails.

Figure 2: Control Center High Availability configuration



Related concepts

About High Availability Management Servers on page 511

Complete the Control Center setup checklist

Use this checklist to set up your Control Center so that it is registered and fully operational. Mark off each step as you complete it.

Setup checklist
1. Plan your configuration
Read the latest Release Notes for up-to-date information. Plan your integration schedule.
2. Set up the Client application
Make sure that you have a Windows-based computer that meets the minimum requirements. Install the Client application software on the Windows-based computer by using the installation USB drive or the *Client CD*. See the *Forcepoint Sidewinder Control Center Product Guide* to set up the Control Center users and roles. Use the Sidewinder Control Center Initialization Tool to create your initial configuration file (ccinit.txt) and save it to your configuration USB drive. **Note:** Load the 5.3.1 ccinit file to the 5.3.2 Sidewinder Control Center Initialization Tool. Modify the file and create a new USB installation configuration file.
3. Set up the Management server
Set up the hardware. 1) Make sure that the Control Center Management Server is properly situated in your network. 2) Connect the power cord and the network cable. 3) Insert the configuration USB drive into the appropriate port. 4) Turn on the Control Center Management Server. 5) After the Control Center Management Server has been configured, remove the configuration USB drive that contains the ccinit.txt file. 6) From your Client application computer, ping the IP address of the Control Center Management Server to verify connectivity. If the ping fails, perform network troubleshooting before continuing with the setup process.
4. Start managing your firewalls

Setup checklist

Log on to your Control Center Management Server.
Use the appropriate Control Center, or Admin Console, or Sidewinder Quick Start Wizard to register the firewall with the Control Center Management Server.

> **Note:** If you need to upgrade a firewall to a version compatible with Control Center, you must use the Control Center to register the firewall.

You can do this on a firewall-by-firewall basis or you can use the multiple firewall option.

Use the Control Center Client application to retrieve objects from the registered firewalls.

Validate the current policy.

Apply the current policy to the registered firewalls.

Complete the post-setup tasks required by your environment. Example tasks include:

- Update the Management Server and the managed firewalls to the latest version.
- Create Control Center users.
- Set up configuration domains.
- Set up any alerts and reports required by your security policy.

Complete the integration schedule checklist

This sample checklist can help prepare and schedule your Control Center integration tasks. Adequate preparation greatly reduces the disruption to your production network.

Support staff and materials considerations

- **Schedule network experts** who are familiar with your existing network components to be available during installation.
- **Schedule firewall experts** who will interact with the Control Center Management Server to be available during installation.
- **Locate any manuals or documentation** that can be useful if problems are encountered.

Network services 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, the physical installation of the Management Server, and for testing critical features and services.

  Note: An experienced Control Center installer requires approximately one full workday to complete the installation, configuration, and testing of a basic installation. Adjust this amount accordingly, based on your experience level and the complexity of your security policy and test plan.

- **Determine whether the managed firewalls need to be upgraded.** If the managed firewalls require a software upgrade to reach a version that is compatible with the Control Center version, your network will experience a brief disruption.

  Note: Only 7.0.1.0.3 and higher firewalls can be managed by Control Center 5.3.2.

- **Tell your users and help desk** the times when the network will be unavailable. Also advise your users about any new access controls that might affect their use of the network.

Port configurations for network communication

The following ports are required for proper communication between the Control Center Management Server and Client application and also between registered firewalls and a standalone Management Server.

Note: These ports must be configured before any communication is attempted between any firewall and the Control Center Management Server.

Table 1: TCP port configurations that are required for network communication

Port	Description
Control Center Management Server to firewall	
Port 9005	Firewall SSL port for the Control Center
Firewall to Control Center Management Server	
Port 7080	Control Center Management Server HTTP port
Port 9005	Control Center Management Server HTTPS/SSL port
Control Center Client to Control Center Management Server	
Port 9005	Control Center Management Server HTTPS/SSL port
Port 5432	Control Center Management Server database

Additionally, the following ports are optional, but must be configured for the specified features.

Table 2: Feature-specific optional TCP port configurations for network communication

Port	Description
Control Center Management Server to firewall TCP ports	
Port 22	Required for SSH communication for firewall registration by using the Add New Firewall Wizard
Firewall to Control Center Management Server	
Port 22	SCP transfers of scheduled firewall configuration backups
Port 9006	Control Center utt_server (program for receiving Secure Alerts)
Port 9009	Control Center utt_server (program for receiving real-time audit from firewalls)

CHAPTER 3

Install the Client application

Contents

Install the Control Center Client application and prepare the configuration data for the Control Center Management Server to manage the firewalls in your network.

Configuration overview

Setting up Control Center includes installing software, configuring the Control Center Management Server, and registering firewalls.

The high-level steps for configuring your Control Center are:

1) Install the Control Center Client application and the Sidewinder Control Center Initialization Tool.
   Use the Client application to administer the Control Center Management Server. Use the Sidewinder Control Center Initialization Tool to create the initial configuration file.

2) Create and save an initial configuration file.
   The Management Server uses this file to obtain basic networking and administrator account information.

3) Turn on the Control Center Management Server and apply the initial configuration.

4) Connect to the Management Server from the Client application.

5) Add firewalls to the Control Center.

Install Control Center software

You can install the Control Center Client application and Sidewinder Control Center Initialization Tool on a Windows-based computer.

As of the version 5.0.0 release of the Control Center Client application, you can install multiple versions of these applications on the same computer. If you have a previous version of these applications already installed, you have the following choices when you go through the installation:

- You can upgrade the previously installed version to this version.
- You can keep your old version and install this version to another location on your computer.

Steps

1) Log on to the Windows-based computer as an administrator.

2) Insert the installation USB drive into a USB port. The **Welcome** window is displayed.

   Tip: Alternatively, you can use the *Client CD* instead of the installation USB drive.

   Note: If the installation program does not automatically start, use Windows Explorer to view the contents of the CD or USB drive, then go to the client folder and double-click the executable (.exe) file.

3) Follow the on-screen instructions.

   Tip: For option descriptions, press **F1**.

   - If you have already installed another version of the Control Center Client application or Sidewinder Control Center Initialization Tool on this computer, make a decision about whether you want to overwrite your old versions or install the new versions at a different location. Make your selections and click **Next**.
   - Accept the default settings when possible and click **Next** until the wizard is complete.

   The Client application and Sidewinder Control Center Initialization Tool are now installed.

4) [Conditional] If you do not have the correct version of Microsoft™ .NET Framework installed, you must install it before you access the Client application. You have the following choices:

   - If you are a new customer, this application is located on the *Client CD* in the Microsoft .NET folder.
   - If you are an upgrade customer, see Knowledge Base article 10575 for instructions on obtaining this version of Microsoft .NET Framework.

Create the initial configuration file

You can create the initial configuration file with the Sidewinder Control Center Initialization Tool.

You can install and use the Sidewinder Control Center Initialization Tool to create a ccinit.txt configuration file for use during the Management Server installation. Instead you can manually configure or use a ccinit.txt from an earlier installation like 5.3.1 to install and configure the Management Server.

Steps

1) Insert your USB drive into one of the USB ports on the computer that contains the Client application.

   Note: Use a different USB drive than the installation USB Drive that was included with your Control Center Management Server.

2) Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Control Center Initialization Tool**.

3) Use the Sidewinder Control Center Initialization Tool to specify configuration information for your Control Center Management Server.

   On each window, complete the required fields. When all of the required fields on a window have been completed, click **Next** to advance to the next window.

   Tip: For option descriptions, press **F1**.

   Note: Initial configuration allows you to set up only one interface. You can add or edit the interface selection and configuration from the Client application.

4) On the **Complete** window, click **Save As** and save the file to the USB drive. Name the file *ccinit.txt*.

   Note: The configuration file must be in .txt format. In the **Save as type** field, select **Text File (*.txt)**.

5) Close the Sidewinder Control Center Initialization Tool.

6) Remove the USB drive.

Result

You are now ready to configure the Management Server.

Apply the configuration file to the Management Server

You can automatically install the Management Server using the initial configuration file. Use the ccint.txt file created from the 5.3.2 Sidewinder Control Center Initialization Tool or a loaded and modified 5.3.1 ccinit.txt file to initialize the Management Server.

Refer to the prerequisites in *Manually configure the Management Server*.

Steps

1) Use a diagram of your network to determine the proper place for your Management Server. Your server must be able to reach the appropriate routers, subnets, and managed firewalls.

2) Attach the power cord to your Management Server and plug it into an electrical outlet.

> **Note:** If your Management Server 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 the network cable.

4) Insert the configuration USB drive into a Management Server USB port.

5) Turn on the Management Server.

   The Management Server automatically loads the configuration information. When the initial configuration is complete, a logon prompt is displayed.

Result

The Management Server now has its initial configuration.

Connect to the Management Server

You can connect to the Management Server using the Client application.

> **Note:** This procedure assumes you are logging on to Control Center for the first time.

Steps

1) Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Sidewinder Control Center**.

2) Specify the appropriate information.

   > **Note:** If another version of the Control Center Client application is installed on this computer, the default information from that version is displayed in this window. Make whatever changes are necessary.

   If this is the first version of the Control Center Client application that is being installed on this computer, you must complete the fields on this window.

   - In the **Name** field, specify a name that quickly identifies this Management Server.
   - In the **Server address** field, specify the host name or IP address of the Management Server.
   - Select **Primary server**, and then complete the following fields with information appropriate for this Management Server:
     - In the **User name** field, specify a valid user name.
     - In the **Password** field, specify the password that has been assigned to this user name by the system administrator.

3) Click **OK**. A **Certificate Problem** message is displayed. The message is similar to the following example:

```
The Management Server's SSL certificate needs to be validated. The server detected the
 following error when contacting the URL "https://<IP_address>:9005/cm/certdist/ca.cer": "A
 certificate chain processed, but terminated in a root certificate which is not trusted by the
 trust provider". Do you want to ignore this error and continue?
```

This message is expected. It is displayed because the application imports a non-Certificate Authority (CA) certificate before it imports the CA certificate of the Management Server. You can safely ignore this error.

4) Click **Yes**. A **Security Warning** message is displayed. The message is similar to the following example:

```
You are about to install a certificate from certification authority (CA) claiming to represent
 CommandCenter CA
```

```
Windows cannot validate that the certificate is actually from "CommandCenter CA". You should
 confirm its origin by contacting "CommandCenter CA". The following number will assist you in
 this process: Thumbprint (sha1): <actual certificate thumbprint>
```

```
Warning:
```

```
If you install this root certificate, Windows will automatically trust any certificate issued
 by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you
 click "Yes", you acknowledge this risk. Do you want to install this certificate?
```

5) Click **Yes**.

If the Management Server and the Client application are the same version, the main logon window is displayed, and the newly created server is selected.

- **Management Server older than the Client** — If the Management Server is older than the Client application, a version warning is displayed when you attempt to log on. Click **Yes**.

  After you have finished your update, restart the Client application.
- **Client older than the Management Server** — If the Client application is older than the Management Server, a Client Software Update prompt is displayed when you attempt to log on. Click **Yes** to begin installing the Client application update.

  Note: The prompt is displayed only if a Client Software Update is available for download from the Management Server.

  After you have finished your update, you are returned to the main logon window.

6) In the **User Name** field, type a valid Control Center user name.

7) [Optional] Click **Remember User Name** to preserve the entered user name in the field for subsequent logon attempts.

8) In the **Password** field, type the password that was assigned to this user name by the system administrator.

9) Click **Connect**. The **Certificate validation** message is displayed. The message is similar to the following example:

```
The Management Server's SSL certificate needs to be validated. When contacting the server at
 the address: nn.nn.nnn.nnn, the server presented a certificate with the following information:
 Subject Name: CN=example.example.net Issuer: CN=CommandCenter CA Expiration: (date)
 (time)Thumbprint: (thumbprint)Do you want to allow communication with this server?
```

10) Click **Yes**.

Result

You are now logged on to the Client application, which is connected to the Management Server.

Add firewalls to the Control Center

Register firewalls with the Control Center Management Server. Depending on the current status of the firewall, you can register multiple firewalls at once, or each firewall individually.

Add multiple firewalls at one time

You can sign up one or more firewalls by initiating the process from the Control Center Management Server, rather than from the firewall. This process can be initiated only under specific conditions and only for specific firewalls that have been prepared to employ this option.

Before you begin

The firewalls must be configured for rapid deployment.

You can also import a prepared file for multiple firewalls to avoid manually specifying the details that are required to support this option. To use this feature, all the firewalls must have the same password.

Sign up multiple firewalls by using the **Sign Up Firewalls** window.

Note: After you complete this task, you will still have to register each firewall separately as an additional task. To add and register a single firewall in one wizard, use the **Add New Firewall Wizard**.

To add multiple firewalls at one time:

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, right-click the **Firewalls** node and select **Sign Up Firewalls**. The **Sign Up Firewalls** window is displayed.

3) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

4) Click **OK** to start the registration process. View the progress of the firewall enrollment process on the **Deployment Status** page.

Add a single firewall

After the Control Center Management Server has been installed and the firewall-specific, Control Center-enabling configurations have been made, you can begin to add new firewall objects and their associated configuration objects to the Control Center Management Server database.

You can add and register a new firewall to the Control Center by using the **Add New Firewall Wizard**. You can also retrieve the configuration from the firewall.
To use this wizard, the Control Center must be able to have SSH access to the firewall. You must configure this SSH access on the firewall. Use the Forcepoint Sidewinder Admin Console to enable the SSH access control rule on this firewall for external sources and destinations. After you save this change, you can come back to the Control Center Client application and run the **Add New Firewall Wizard**.

Creating firewall objects is a two-part process:

1) All types of firewall objects that represent physical devices in your configuration must be identified by providing basic information.

2) All the firewall-specific configuration information must be created or retrieved for each firewall.

Both of these parts can be performed in the **Add New Firewall Wizard**. You can use the **Add New Firewall Wizard** as described in the following examples:

- You have already added several firewalls by using the **Sign Up Firewalls** window. Now you need to retrieve their configurations. Perform a retrieve for each firewall individually with this wizard.
- If a single firewall is not registered with the Control Center, you can add it, register it to Control Center, and retrieve its configuration—all in one step.
- If a single firewall has already been registered with the Control Center, you can add it and retrieve its configuration.

Note: If a firewall has already been added to and registered with the Control Center Management Server, you can retrieve its configuration by using the **Firewall Retrieval Options** window.

Steps

1) In the navigation bar, select **Policy**.

2) To display the **Add New Firewall Wizard**:

   - In the **Policy** tree, double-click the **Firewalls** node.
   - Right-click the **Firewalls** node and select **Add Object**.

   Tip: For option descriptions, press **F1**.

3) To begin the process of adding the firewall to the list of firewalls in the **Policy** tree, complete the information on the **Firewall Connection Information** page and click **Next**. The **Firewall Registration Information** page is displayed.

4) Select an option to register the firewall with the Control Center Management Server.

   To skip the registration process, on the **Firewall Registration Information** page, click **Next**. The **Retrieval of the firewall into Control Center** page is displayed. Skip to Step 7.

   To register this firewall with the Control Center Management Server:

   a) On the **Firewall Registration Information** page, select the **Register the firewall with this Management Server** checkbox.

b) Click **Next**. The **Summary** page is displayed.

5) On the **Summary** page, verify the information that you have configured. If it is correct, click **Register**; if not, correct any problems. The **Registration Status** page is displayed.

6) On the **Registration Status** page, view the progress of the firewall registration. After it successfully completes, click **Next**.

7) To retrieve items and categories from the firewall into Control Center, on the **Retrieval of the Firewall into Control Center** page, select the items and categories to be retrieved and click **Finish**. These objects are retrieved and the firewall is displayed in the list of firewalls in the **Policy** tree.

Add an HA cluster

You can register a standalone firewall or a High Availability cluster that already has a configured policy.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, right-click the **Clusters** node and select **Add Object**. The **Add New Cluster Wizard** window is displayed.

3) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

4) Click **OK** to start the registration process. View the progress of the firewall enrollment process on the **Deployment Status** page.

Perform post-setup tasks

Set Tomcat Java heap size for better performance.

1) As a root user run the command:

```
vi /usr/local/tomcat/bin/setenv.sh
```

> **Note:** The value in `setenv.sh` must be in multiples of 128. We recommend that for large configurations, you set this value to 1024 .

2) Look for the `JAVA_OPTS` property, which will be set something like below, the number highlighted below are the variables which depends upon configured RAM size.

```
JAVA_OPTS="-Xms 499 m -Xmx 499 m"
```

3) Follow below table to set this JAVA_OPTS for better performance and replace it accordingly based on RAM size.

RAM Size	JAVA_OPTS Value to set
1 GB	JAVA_OPTS="-Xms512m -Xmx512m"
2 GB	JAVA_OPTS="-Xms1024m -Xmx1024m"
3 GB	JAVA_OPTS="-Xms1536m -Xmx1536m"
4 GB	JAVA_OPTS="-Xms2048m -Xmx2048m"
6 GB	JAVA_OPTS="-Xms3072m -Xmx3072m"

4) Restart the tomcat by running below command as a root user.

```
service tomcat restart
```

Note: The Java settings are automatically configured with the correct.memory.sh script during installation.

Attention:
In the following complex scenarios, the settings might need further tuning and we recommend you to increase JAVA_OPTS by multiples of 128. For example, if you have a complex nested rule deployment with 3500 rules with carried over nested groups and Control Center (2GB Physical RAM and 1024m JAVA_OPTS). Control Center is throwing an Out of Memory or a GCC overhead error. So it is recommended you increase the JAVA_OPTS to 1024m+(128*2=256m)=1280m

- Continuous GCC overhead error
- Out of memory error in the CC logs or catalina logs
- Large number of rules, example beyond 2500
- Lot of nesting in the rules
- Lot of nested groups that might have come in the rules during firewall upgrade from older versions of firewall like 7x to 8x

Related tasks

Download and apply Management Server updates on page 527
Back up your configuration files on page 469
Configure HA Management Servers on page 517

Related information

Configure Control Center administrators on page 490

CHAPTER 4

Navigate the Control Center user interface

Contents

The Control Center Client application is designed to provide a centralized location from which you can perform all the tasks that you need to manage your security policy and firewalls in your distributed network environment.

Working with Management Servers

This section explains how to log on to, add, or delete Management Servers.

Log on to the Management Server

Launch the Client application and log on to the Control Center Management Server.

Steps

1) Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Sidewinder Control Center**.

2) Specify a valid Control Center user name in the **User Name** field. After the initial installation of the Management Server, the default user name is the Control Center administrator user name specified in the ccinit.txt file.

3) [Optional] Select the **Remember User Name** checkbox to preserve the specified user name in the field or the default user value that is specified in the ccinit.txt file.

4) Specify the corresponding password in the **Password** field.

5) Select a Management Server connection from the **Server** list or select **<Add New Server>** to add a new Management Server connection.

6) Click **Connect**. A certificate validation message is displayed.

7) Click **Yes**.

Result

You are now logged on to the Management Server.

> **Note:** If you attempt to log on to a Management Server using a Client application version earlier than the Management Server version, you will be prompted to update the Client application before proceeding.

Add a backup (standby) Management Server

Configure a secondary, or backup, Control Center Management Server.

Steps

1) Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Sidewinder Control Center**.

2) Specify the user name and password in their respective fields.

3) In the **Server** field, make sure that **<Add New Server>** is displayed and click **Browse**. The **Add New Server** window is displayed.

4) Configure the fields in this window, specifying whether you are adding a primary or a backup (standby) server and then specifying the related field information.

5) Click **OK**. The **Certificate Problem** message is displayed because the Management Server imports a non-Certificate Authority (CA) certificate before it imports the CA certificate. Click **Yes**. Another message is displayed. Click **Yes**. The logon window is displayed.

6) In the **Server** list, select the server to log on to. Then specify the user name and password for that server and click **Connect**.

Remove Management Servers

Use this procedure to delete a Control Center Management Server from the list of Management Servers.

Steps

1) Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Sidewinder Control Center**.

2) Specify the user name and password in their respective fields.

3) In the **Server** field, select the server to be removed and click **Browse**. The **Add New Server** window is displayed.

4) Click **Remove**.

Result

The Management Server is removed from the list of available Management Servers.

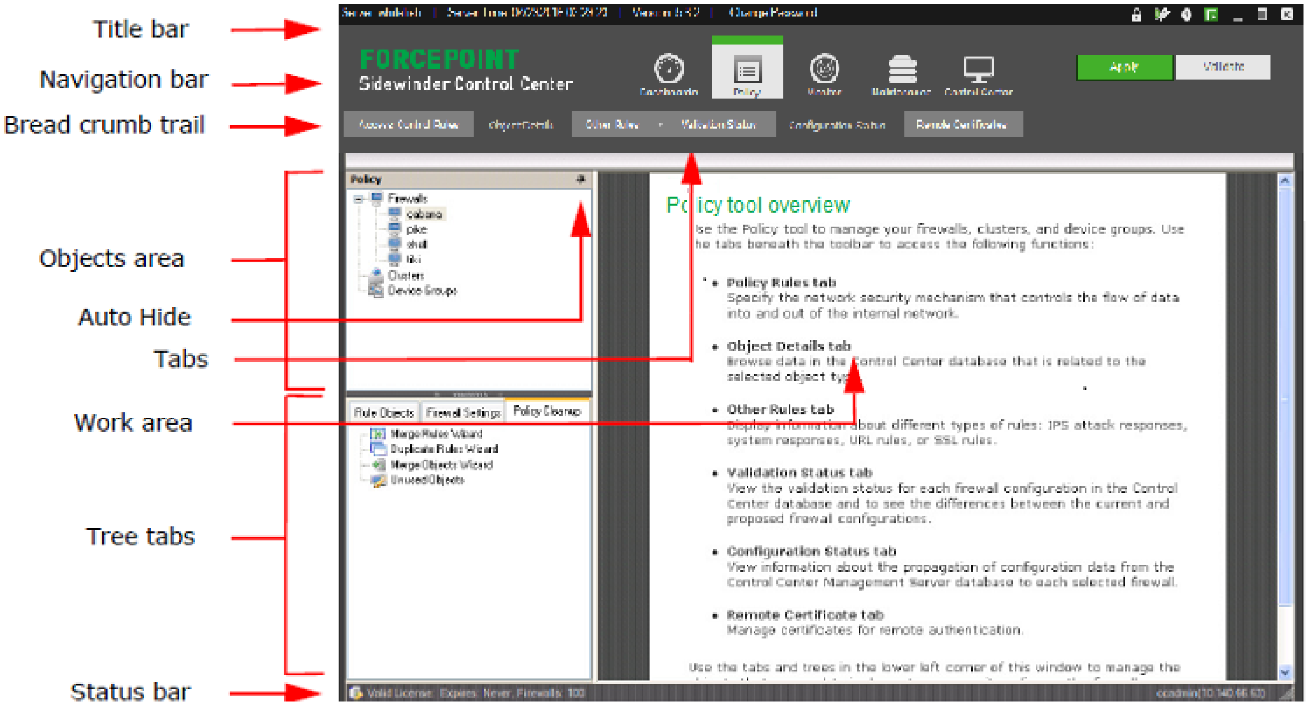
User interface overview

The Control Center Client application interfaces consists of links, icons, buttons, tabs, trees, and displayed information, such as server information and the users who are logged on to this configuration domain of this Management Server. (If no configuration domains are implemented, everyone is logged on to the default domain.)

The Control Center Client application is displayed after you have successfully logged on to the Control Center Client.

The following figure shows the different areas that make up the Control Center Client application.

Figure 3: Example of the Control Center Client main window



Policy tool overview

Use the Policy tool to manage your firewalls, clusters, and device groups. Use the tabs beneath the toolbar to access the following functions:

- **Policy Rules tab**
  Specify the network security mechanism that controls the flow of data into and out of the internal network.
- **Object Details tab**
  Browse data in the Control Center database that is related to the selected object type.
- **Other Rules tab**
  Display information about different types of rules: IPS attack responses, system responses, URL rules, or SSL rules.
- **Validation Status tab**
  View the validation status for each firewall configuration in the Control Center database and to see the differences between the current and proposed firewall configurations.
- **Configuration Status tab**
  View information about the propagation of configuration data from the Control Center Management Server database to each selected firewall.
- **Remote Certificate tab**
  Manage certificates for remote authentication.

Use the tabs and trees in the lower left corner of this window to manage the

Title bar

The title bar is located across the top of the main window.

Server-related information

The information in this left portion of the title bar provides information about the Management Server and also a link for changing the password that you use to access this server.

Table 3: Server-related information

Option	Definition
Server	Displays the name of the Management Server to which you are logged on.
Server Time	Displays the current date and time of the Management Server to which you are logged on.
Version	Displays the current version of the Management Server to which you are logged on. This value is the same as the value of the Management Server Version field on the **About Forcepoint Sidewinder Control Center** window.
FIPS 140-2 processing enabled	Appears if FIPS 140-2 cryptography processing is enabled on the Control Center.

Option	Definition
Change Password	Displays the **Change User Password** window, where you can change your user password. This window is available only if your user profile has been configured to use internal authentication to access the Control Center. If you have administrator privileges and you want to change the password of a different user, use the **Control Center Administrator** window.

Title bar icons

There are several functions are provided by the icons located to the right in the title bar.

- **Locking objects to protect single user updates** — Protect selected objects from being simultaneously updated by multiple users by clicking **Locking Manager** on the title bar. The **Locking Manager** window is displayed, where you can select one or more objects to lock for this active session.
- **Starting and stopping a ticket to track changes** — Start a ticket to begin capturing audit data from a specific point in time. This data will be identified on the **Firewall Audit** page by the ticket number that you have assigned to this ticket. After you have started a ticket, you can stop it at any time. Perform this function by clicking (**Start ticket**) or (**Stop ticket**).
- **Accessing online Help** — Access the main Help page from anywhere in the Client by clicking **Help**. You can access window- or page-specific online Help by pressing **F1**.
- **Accessing Control Center version information** — Access information about the Control Center, such as Client, Management Server, and database versions and copyright information by clicking **About**.

Navigation bar

Several icons are located in the navigation bar area of the main window.

- Dashboards
- Policy
- Monitor
- Maintenance
- Control Center

The information that is displayed in the tab area, bread crumb area, objects area, and work area is specific to the icon that is currently selected.

Additionally, there are two buttons in the navigation bar area:

Table 4: Navigation bar area buttons

Option	Definition
Apply	Applies configuration changes to one or more firewalls. You can also apply changes for a specific firewall by right-clicking it in the **Policy** tree and selecting **Apply Configuration**.
Validate	Validates configuration changes to one or more firewalls. You can also validate changes for a specific firewall by right-clicking it in the **Policy** tree and selecting **Validate Configuration**.

Tabs

Each icon has its own set of tabs that provide access to additional functions. When selected, a tab either displays the related page in the work area or it displays a menu from which you can select additional pages.

For more information about the tabs and their menus, see the section for each icon.

In addition to these icon-specific tabs on the left part of this area, when configuration domains have been activated, the following fields and buttons are displayed, regardless of the icon that is currently selected:

Table 5: Additional fields and buttons

Option	Definition
Domain	Displays the list of configuration domains. You can change to a different domain, provided that you have access to it, by selecting it in this list. The displayed domain is the domain to which you are logged on.
Manage versions	Displays the **Manage Configuration Domain Versions** window, where you can create, modify and activate versions of a configuration domain.

Related concepts

Advantages of configuration domains on page 499

Bread crumb trail

Whenever a tab is clicked or a menu option from a tab is selected, the title of the page is displayed in the bread crumb trail.

If the page that is displayed is the result of a menu selection, the entire bread crumb is displayed in the bread crumb trail. For example, on the **Monitor** icon, if you click **Reports** and then select **Policy Report**, the bread crumb trail displays **Reports** > **Policy Report**.

Object area

The object area can differ from icon to icon, depending on whether the icon has any object trees or tabs.

Trees

Some of the icons provide the ability to configure objects that are found in a tree view that is located in the object area.

The most complex icon is the **Policy** icon, with its firewall tree at the top of the object area and a set of tabs, each with its own tree at the bottom of the object area. The **Monitor** icon currently does not have an object area.

Auto Hide button

For every icon that has an objects area, there is also the **Auto Hide** button. Use this button to manage the display (or hiding) of the **Objects** area to increase the size of the work area in the main window.

To hide the objects area, click the **Auto Hide** button. To bring back the display of the objects area, click the object area name on the left to display the object area. Then click the **Auto Hide** button to lock it into its original position.

Tree tabs

Because there are many configuration objects that can be configured on the **Policy** icon, the bottom of the objects area is broken out into tabs, each with its own tree of objects to be configured.

Work area

This portion of the user interface is where the data that is associated with the pages is displayed when the associated tab for the page is selected.

Status bar

The status bar at the bottom of the main window displays information about users.

Table 6: Status bar information

Option	Definition
Users	Displays the name and the IP address of each user who is currently logged on to the current domain of the Management Server. This information is in the right corner of the status bar.

Additional navigational aids

There are additional functions that are provided in the Control Center Client to help you configure and manage the security policy for your firewalls.

- **Right-click menus** — Right-click menus are available for the objects that appear in the trees in the Objects area. You can also use the right-click menu in some of the pages that are displayed in the work area, such as the Access Control Rules page. Many of these menu options are also accessible through another way on the page, such as a tool on the toolbar for the page.
- **Edit status column** — Many tables that are displayed on windows and pages include the first column, which is an Edit column that identifies the edit status of a row in a table. The following icons can be displayed in this column:
  - **[blank]** — Indicates an existing line with associated values that is not the currently selected line.
  - **Edit** — Indicates that this row is the one that is being edited.

- **New** — Indicates that you are creating a new row or entry.
- **Current** — Indicates that this row is currently selected and it contains previously specified values.

Search for objects in the Control Center Client application

You can search for configurable objects within a larger list of objects by specifying certain criteria in the **Search** window.

Often, the name that is associated with an object is not enough information to identify the object that you need to find. By using the **Search** window, you can specify any character or string of characters to search through all the presented data columns to locate the item that you seek.

Steps

1) From various lists in windows and pages, click **Search**. The **Search** window is displayed.

   Tip: For option definitions. press **F1**.

2) Enter a search term, then click **Filter**. Items in the list that contain the search term are displayed in a drop-down list.

3) Select the item you were looking for.

Result

The item is selected (checkbox filled with a check mark) in the list.

Client application icons

Icons are provided for common tasks.

Most icons have tooltips that appear when you hover your mouse over them.

Table 7: Client application icons

Icon	Description
Common icons	
	Apply
	Delete
	Edit
	Help

Icon	Description
▶	Line Selection
🔒	Locking Manager
🔄	Refresh
⚠	Version Warning
❗	Warning
⚙	Validate
Search icons	
	Clear Search
🔍	Search
Status icons	
🔴	Status: Not Running
🟢	Status: Running
🟡	Status: Uncertain
?	Unknown Status
Policy Tree icons	
🖥	Firewalls
	Crossbeam firewall
	Clusters
	Device Groups
Rule Object icons	
👤	Users
👥	User Groups
	External Groups
	McAfee® Logon Collector Users

Icon	Description
	McAfee Logon Collector Groups
	McAfee Logon Collector Distribution Lists
Rule icons	
	Add Rule
	Edit Rule
	Delete Rule
	Delete Rules
	Move to Position
⇩	Move Down
⇧	Move Up
	Search and Replace
	Export Rule
	Rule
	Rule Group
Alerts icons	
♫	Alarm Sound Mapping
✓	Acknowledge
	Alert jump
	Alert options
	Annotate
	Clear
●	Critical
●	High
●	Medium

Icon	Description
●	Low
●	Warning
	Export to CSV
⚠	Secure Alert Server status
	View events
✚ ⊕ ⊕	Add
	Administrators
Update icons	
	Update Settings
	Schedule Firewalls
	Manual Download
Control Center Tree icons	
	Administrators
	Roles
	LDAP User Groups
📌	Auto-Hide
...	Browse
⊗	Clear Filter
	Clear Pending Changes
⊟	Collapse All
⊞	Expand All
	Manage Configuration Domain
⇩ ⇩	Move Down

Icon	Description
⇦	Move Left
⇨	Move Right
⇈	Move to Top
⇧ ⇧ ⇧	Move Up
💾	Save Pending Changes
⛔	Service Not Running
➡	Service Running
⚠	Service Running Error

PART II

Policy

Contents

Configure and distribute rules and security settings to the firewalls on your network.

CHAPTER 5

Policy overview

Contents

Rules provide the means for applying policy from the Control Center Client application onto the firewall. They determine the way that the firewall processes network traffic.

Types of rules

In the Control Center Client application, the following types of rules are available.

- **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.
- **Attack responses** — Determine the way that the firewall will react when it detects audit events that indicate potential attacks.
- **System responses** — Determine the way that the firewall will react when it detects audit events that indicate significant system events.
- **URL Rules** — Redirect inbound HTTP connections based on application data.
- **Alert processing rules** — Determine how the firewall handles alerts.

Related concepts

About alert processing rules on page 365

About responses on page 185

How URL rules work on page 314

How access control rules work on page 297

How SSL rules work on page 311

About the Policy icon

Use the trees and tabs of the **Policy** icon to define, configure, and maintain multiple firewalls and security policies (access control rules) for a distributed homogeneous or heterogeneous configuration of firewalls.

Access control rules are applied to all traffic that flows into and out of firewalls. Each access control rule is a definition of criteria that are used to inspect incoming or outgoing traffic. Access control rules determine whether this traffic will be allowed to continue to its destination. This section introduces the different ways traffic can be directed through or into the firewall.

You can accomplish the following tasks by using the features and functions of the **Policy** icon:

- **Create configurable rule objects for access control rules** — The components that comprise a security policy include a set of configurable objects that defines the characteristics of the building blocks that are used to implement the security policy. Use this object model of defined objects to share characteristics, options, and functions, instead of having to provide raw configuration information for each aspect of an implemented security policy. Use the **Policy** icon to retrieve, create, and manage configurable object characteristics.
- **Manage configurable rule objects** — After rule objects have been defined or retrieved, you can edit, validate, and apply changes to the configured object. You can manage the implemented security policy across all the supported firewalls in your configuration.
- **Create and manage access control rules** — Access control rules provide the network security mechanism that controls the flow of data into and out of the internal network. They specify the network communications protocols that can be used to transfer packets, the hosts and networks to and from which packets can travel, and the time periods during which the rules can be applied. Access control rules are created by the system administrator and should reflect the internal network site's security policy. Depending on the requirements of your configuration, there might be from hundreds to tens of thousands of rules to manage. Use the **Access Control Rules** tab to view and manage these rules.
- **Create setting objects for firewalls** — There is a different set of configurable objects that can be used to help define one or more firewalls. These objects are located on the **Firewall Settings** tab of the **Policy** icon.
- **Manage setting objects for firewalls** — You can manage these firewall setting objects as standalone entities or you can manage them from within the **Firewall** or **Cluster** window. You can also drag existing objects from the **Firewall Settings** tree to the firewall or cluster in the **Policy** tree.
- **Register and manage firewalls** — Firewalls represent the physical devices that are used to implement a security policy for an organization. They are designed to protect organization IT infrastructure by keeping out unauthorized users, code, and applications, both internally and externally. You can retrieve the settings of existing firewalls or you can configure new firewalls in the **Policy** tree.
- **Maintain access control rules and objects** — Several features are available to help you maintain your list of access control rules, rule objects, and firewall objects. You can combine similar objects or delete duplicate access control rules or objects that are not being used anywhere. These wizards and windows are located on the **Policy Cleanup** tab of the **Policy** icon.

Related concepts

Configurable firewall objects on page 191
Policy cleanup nodes on page 373
About policy objects on page 55

Policy icon operations

The **Policy** icon hosts the following operations outside of the **Policy** area in the interface.

Table 8: Tabs for the Policy icon in the navigation bar

Tab	Definition
Access control rules	Displays the **Access Control Rules** page, where you can manage the access control rules that control the flow of data into and out of the network.
Object Details	Displays the **Object Details** page, where you can browse object-specific data in the Control Center database that is related to the object type that has been selected in one of the trees of the **Policy** icon.

Tab	Definition
Other Rules	Displays the following options: • **SSL rules** — Displays the **SSL Rules** page, where you can configure the Secure Sockets Layer (SSL) parameters, such as keys and certificates, for decrypting a session. • **Attack Responses** — Displays the **Attack Responses** page, where you can configure and modify attack responses. Attack responses define the way that the firewall responds when it detects audit events that indicate such possible attacks as Type Enforcement violations and proxy floods. • **System Responses** — Displays the **System Responses** page, where you can configure and modify system responses. System responses define the way that the firewall responds when it detects audit events that indicate such significant system events as license failures and log overflow issues. • **URL rules** — Displays the **URL Rules** page, where you can configure the redirection of inbound HTTP connections, based on application layer data, rather than on transport layer data that is used for the conventional redirect rules.
Validation Status	Displays the **Validation Status** page, where you can view and validate changes that were made to a firewall configuration by using the Control Center Client. These changes were made to the data that is stored on the Management Server. These changes can then be viewed and validated against the previously applied configuration.
Configuration Status	Displays the **Configuration Status** page, where you can view the various status conditions for configuration changes that are being applied to firewalls. After configuration changes have been made to a firewall, they must be applied to the appropriate firewall. This process is initiated by clicking **Apply Configuration** in the main area.
Remote Certificates	Displays the **Remote Certificates** page, where you can manage remote certificates. You can also request, load, retrieve, view, export, and delete certificates on this page.

CHAPTER 6

Policy objects

Contents

In the **Policy** icon of the Forcepoint Sidewinder Control Center Client application, all the objects related to policy are divided into three different groups. These groups are represented by the three different tabs, **Rule Objects**, **Firewall Settings**, and **Policy Cleanup** in the lower left portion of the main window when the **Policy** icon is selected.

About policy objects

You can define various components that are used to implement a security policy on the tabs of the **Policy** icon. The components are comprised of a set of configurable objects that encapsulate the characteristics of each of the individual building blocks.

Using this object model, the defined objects are used to share characteristics, options, and functions instead of having to provide raw configuration information each time an individual component is created.

You can define objects and apply them in various situations, such as access control rules, while retaining the ability to change the characteristic of an object without having to locate and change every instance.

For example, an address object can be defined that identifies a fixed set of addresses that use a base address and an address mask. This object can represent a group, division, or some other organizational characteristic that is associated with an enterprise. An entire set of access control rules can then be defined that use this object as a source or destination for a specific type of packet traffic. Eventually, dozens or even hundreds of rules can be defined to manage proxies and other services can be developed that use this network object as a source or destination address. When you need to change the addressing because the organization made a move, or for any other network-related reason, the base address and mask characteristics of the network object can be changed and automatically applied to all the associated access control rules.

Types of rule objects

The basic set of configurable objects for access control rules consists of several objects.

- **Network objects** — Specify source or destination conditions in access control rules. The following categories of endpoint objects are defined on the firewall:
  - **Hosts** — Specify a fully qualified host name or an IP address
  - **Networks** — Specify an entire sub-network to use as an endpoint.
  - **Address Ranges** — Specify an inclusive series of IP addresses. You can specify a portion of a sub-network to use as an endpoint.

  - **Domains** — Specify a domain to use as an endpoint.
  - **Adaptive** — Specify an adaptive endpoint, which is a single endpoint that can be used in different ways by multiple security firewalls.
  - **Geo-Location** — Specify a list of countries that are defined in a Geo-Location object to use as an endpoint.
  - **Zones** — Specify a zone to use as an endpoint.
  - **Zone Groups** — Specify a zone group to use as an endpoint.
  - **Net Groups** — Specify and name groups of endpoints by using previously configured endpoint objects and a set of system-wide interface controls.
    Additionally, you can import network objects to use in access control rules.
- **Application Objects** — [Available for firewall version 8.0.0 or later access control rules] Specify a custom application based on existing applications with different port configurations. You can also group together applications to form application group objects that can be used in access control rules.
- **Services** — [Available for firewall version 7.x access control rules only] Specify a network communications protocol. Services are used as conditions in access control rules. The firewall supports the following categories of network services:
  - **Proxy Services** — Specify a network service that is associated with a proxy agent that is running on the firewall. The proxy agent controls communication between clients on one side of the firewall and servers on the other side. The user's client program communicates with the proxy agent instead of communicating directly with the server. The proxy agent evaluates requests from the client and determines the requests to permit and to deny, based on your security policy. If a request is approved, the proxy agent forwards the client's requests to the server and forwards the server's responses back to the client. The proxy agent is application aware (for example, it understands the application layer protocol and can interpret its commands).
    Proxy agents are used to create proxy services. Proxy services may be TCP-based or UDP-based. Many are defined by default for such TCP-based services as HTTP, FTP, and Telnet and for such UDP protocols as SNMP and NTP. Use the **Proxy Service** window to create additional proxy services.
  - **Filter Services** — Specify a network service that is associated with a filter agent that is running on the firewall. Filter agents provide another way for clients and servers to communicate. The filter agent inspects and passes traffic at the network layer or at the transport layer. The following types of filter agents are provided:
    - **TCP/UDP** — Transport Control Protocol (TCP) is a transport layer protocol that is defined by a specified port number or range of port numbers. User Datagram Protocol (UDP) is a transport layer protocol that is defined by a specified port number or range of port numbers.
    - **ICMP** — Internet Control Message Protocol (ICMP) is a network layer protocol that supports packets that contain error, control, and informational messages.
    - **IP** — Internet Protocol (IP) is a network layer protocol that is defined by a protocol number.
  - **Service Groups** — Specify a collection of network services that are defined on the firewall.
- **Application Defenses** — Specify the settings for inspecting advanced application-level content, such as headers, commands, and filters. They also enable add-on modules such as virus scanning, spam filtering, and web filtering. They can be used with filter services, most proxy services, and the sendmail server service. Additionally, you can create Application Defense groups to use in access control rules.
- **IPS** — Specify IPS response mappings so that you can create and maintain IPS signature groups. You can also use the **IPS Signature Browser** to view and manage IPS signatures.
- **Authenticators** — Specify authentication services that contain the authenticators that are used by the firewall. The following types of authenticators are available:
  - Password
  - Passport
  - RADIUS

  - Safeword
  - Windows Domain
  - iPlanet
  - Active Directory
  - OpenLDAP
  - Custom LDAP
  - CAC

- **Firewall Users** — Specify firewall users who can access the Control Center and the way in which they can access it. User identification and authentication is a critical aspect of security. To access a firewall, a user must have a logon ID and a method of authentication. Users can be configured to have one authentication method for inbound connections and another method for outbound connections.

  The firewall supports multiple methods of identification and authentication. You can use the Control Center to create two classes of users: firewall users (who are defined by using the user objects on the Policy icon) and Control Center users. Firewalls support one or more of the following types of users:

  - **Administrators** — Identifies firewall administrator accounts. A firewall administrator is someone who logs directly into the firewall to perform administrative activities.
  - **Users** — Identifies user accounts to be stored on the firewall.
  - **User Groups** — Identifies internal groups that are used to restrict access to services through the firewall.
  - **External Groups** — Identifies external groups that are used in access control rules to restrict access to services through the firewall.
  - **MLC Users** — [Available for version 8.0.0 or later firewalls] Identifies users who are monitored by the McAfee Logon Collector.
  - **MLC Groups** — [Available for version 8.0.0 or later firewalls] Identifies groups of users who are monitored by the McAfee Logon Collector.
  - **MLC Distribution Lists** — [Available for version 8.0.0 or later firewalls] Identifies e-mail distribution lists that are monitored by the McAfee Logon Collector.

- **Time Periods** — Specify time periods that represent named periods of time. These named time periods are used for various functions, such as limiting the time that a user has the ability to log on to the Control Center or determining the time during which access control rules apply to the assigned firewall.
- **VPN** — Specify a Virtual Private Network (VPN) that securely connects networks and nodes to form a single, protected network. The data is protected as it tunnels through unsecured networks, such as the Internet or intranets. The VPN ensures data origin authentication, data integrity, data confidentiality, and anti-replay protection. A VPN works by encapsulating packets to or from the network with which you want to communicate (the remote network) and by sending them (usually encrypted) as data in packets to or from the network to which you are connected

  The VPN is a security gateway between trusted and non-trusted networks that protects network access, network visibility (NAT), and network data (VPN). The two types of supported VPN connections are gateway-to-gateway and VPN host-to-gateway.

  - **VPN Wizard** — Create VPN channels, including configuration of peers, cryptographic parameters, and the authentication method.
  - **VPN Peers** — Create peer objects that will participate in gateway-to-gateway VPN communities by using the **VPN Peer** window.
  - **VPN Communities** — Configure VPN communities for a firewall by using the **VPN Community** window to configure VPN communities for a firewall.
  - **VPN Client Configurations** — Establish a network configuration for the VPN client to operate on the private side of a firewall by using the **VPN Client Configuration** window.
  - **VPN Bypass** — Select certain traffic to bypass IPsec policy evaluation and to be sent outside of the encrypted tunnel by using the **VPN Bypass** window.

- **CA Certificates** — Import Certification Authority (CA) certificates. A public key certificate is an electronic document that binds a host's identity with its private key. The purpose of a certificate is to provide proof of a host's identity. This enables a secure means of encrypting the data communication between one host and another. In digitally signing the certificate, the Certification Authority (CA) vouches for the host's identification, and is then able to issue a secure certificate that will be used to create a digital signature for the data that is being sent. Use the sender's digital signature, along with the sender's certificate, to verify that (a) the data originated from the sender, and (b) that the data was not tampered with in transit.
- **CA Certificate Groups** — Create CA certificate groups, which consist of one or more CA certificates.

- **SSH Known Hosts** — Specify strong known host associations. You can manage this database that includes only those SSH known host keys with strong trust levels across all firewalls.
- **Audit Filters** — Specify parameters for filtering the audit data so that you can respond to audit events of particular interest to your site in an effective way by using the **Audit Filters** window.
- **Responses** — Specify email accounts that will receive alerts during an attack response and specify hosts from which suspect traffic is to be blackholed, or ignored.

Related tasks

Maintain objects on page 58

Maintain objects

Use the following functions to manage rule objects, firewall objects, and cleanup nodes while you are working in the Control Center Client application.

View object details

You can browse data in the Control Center database that is related to the object type that has been selected in one of the trees of the **Policy** icon in the **Object Details** page.

Note: There is only one **Object Details** page. Every time that you select a different object type, the data that is displayed on this page is overwritten with the data for the newly selected object type.

Steps

1) In the navigation bar, select **Policy**.

2) To view a list (tree) of objects, click one of the tabs in the **Policy** area and then expand one of the object nodes.

3) Click a subnode object in the tree.

4) Click the **Object Details** tab.
   The list of objects appears on the **Object Details** page.

   Tip: For option definitions, press **F1**.

Edit object data

You can edit object data on the **Object Details** page in two different ways.

Steps

1) In the navigation bar, select **Policy**.

2) To view a list (tree) of objects, click one of the tabs in the **Policy** area and then expand one of the object nodes.

3) Click a subnode object in the tree.

4) Click the **Object Details** tab.
   The list of objects appears on the **Object Details** page.

   Tip: For option definitions, press **F1**.

5) Edit object data using one of the following methods.
   - Double-click the object row — The window for that object is displayed. For example, if the object details for all your firewalls were displayed on this page, double-click a particular firewall and the **Firewall** window is displayed with the data for that firewall. You can then change any of the data as required.
   - Right-click the object row — The menu options vary, depending on the object that you are viewing on this page. Possible options include:
     - Adding a new object
     - Editing the selected object
     - Copying the selected object
     - Removing the selected object
     - Showing all the references to this object (**Show Usage**)

Locking configuration objects

Locking a set of objects ensures that no other Control Center user can add, modify, or delete objects of that type.

Multiple Control Center users can be logged onto the same Management Server using multiple Client application clients. This means that, at any given time, multiple users can be making simultaneous changes. To alleviate the possibility of contention, the Control Center provides a mechanism to lock selected objects (for example, address ranges, networks, access control rules) so that other Control Center users cannot simultaneously add, modify, or delete those types of objects.

When you or another user locks a set of objects, the lock status is indicated in the Objects toolbar by highlighting on the name of the object type using a red or blue color. If *you* have locked a set of objects, the name of the object type is displayed with a green highlight. If *another user* has locked a set of objects, the name of the object type is displayed with a red highlight.

The lock that you obtain for a set of objects is temporary; you can activate or unlock the lock at any time. If you do not remove the lock, the lock will be removed automatically when you log off of all client user interfaces that you have logged onto or when all your server sessions expire.

Note: Locks are assigned based on a user name; locks are *not* assigned based on the server session to which you have logged on. This means that explicit locking and unlocking status is reflected in all clients that a user is logged onto. If a user is logged into more than one client, any active locking status is retained until he logs out of every client (or until all sessions expire).

Lock objects

You can lock one or more sets of Control Center objects to prevent multiple users from accessing and changing the same objects.

Steps

1) In the title bar, click **Locking Manager**. The **Locking Manager** window is displayed.

   Tip: For option definitions, press **F1**.

2) Select the checkbox next to all the objects to be locked.

   Tip: To lock all objects, select the **Lock all objects** checkbox.

3) Click **OK** to obtain the locks.

CHAPTER 7

Network objects

Contents

Network objects represent source or destination conditions used in access control rules.

Types of network objects

You can define several different types of network objects.

- **Hosts** — Specify a fully qualified host name or an IP address to configure an endpoint.
  If you have configured the ePolicy Orchestrator to communication with the Control Center, you can also view McAfee ePO data for a specific host.
- **Networks** — Specify an entire subnetwork to use as an endpoint.
- **Address Ranges** — Specify an inclusive series of IP addresses. You can specify a portion of a subnetwork to use as an endpoint.
- **Domains** — Specify a domain to use as an endpoint.
- **Adaptive** — Specify an adaptive endpoint. An adaptive endpoint is a single endpoint that can be used in different ways by multiple firewalls.
- **Geo-Location** — Specify a Geo-Location network object, which is a specified group of country IP addresses.
- **(Security) Zone**s — Specify a zone.
- **Zone Groups** — Specify zone groups.
- **Netmaps** — Specify netmap objects to specify mapping between IP addresses and networks.
- **Net Groups** — Specify and name groups of endpoints using previously configured endpoint objects and a set of system-wide interface controls.
- **Import Network Objects** — Displays the **Import Network Objects Wizard**, in which you can specify a file from which you can import network objects that are defined in that file.

Related tasks
Configure device groups on page 293

Create a host object

You can add a fully qualified host name or IP address endpoint.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Network Objects** node.
4) Double-click the **Hosts** node. The **Host** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description for the object.
6) Specify the object type, and configure any type-specific parameters.
7) Click **OK**.

Result

The new host object is added to the **Hosts** node, and can be used when you configure a rule.

Create a network, address range, or domain object

You can add a network, address range, or domain object.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Network Objects** node.

4) Double-click **Networks**, **Address Ranges**, or **Domains**, depending on the type of object you want to create. The Network Object window for the object appears.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description for the object.

6) Specify the object type, and configure any type-specific parameters.

7) Click **OK**.

Result

The new network object is added to the appropriate node, and can be used in a rule.

Related tasks
Maintain objects on page 58

Create an adaptive endpoint

You can create an *adaptive endpoint*. An adaptive endpoint is a single endpoint object that can be used differently by multiple firewalls.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Network Objects** node.

4) Double-click the **Adaptive** node. The **Adaptive** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description for the adaptive endpoint object.

6) Add firewall-specific addresses as needed.

7) [Optional] Define a default address for unspecified firewalls.

8) Click **OK**.

Result

The new adaptive endpoint object is added to the **Adaptive Endpoint** node, and can be used in a rule.

Create a Geo-Location object

You can create a *Geo-Location* object. Geo-Location identifies the IP address for the country of origin. Use a Geo-Location object in an access control rule to allow or deny a network connection based on the source or destination country.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Network Objects** node.

4) Open the **Geo-Location** window. Do one of the following:
   - Double-click the **Geo-Location** node.
   - Right-click the **Geo-Location node** and select **Add object**.

   The **Geo-Location** window appears.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description.

6) Specify the countries to include in the **Geo-Location** object.

7) Click **OK**.

Result

The new **Geo-Location** object is added to the **Geo-Location** node and can be used in a rule.

Create a security zone

You can create a *zone*. A zone is a type-enforced network area that is used to isolate network interfaces from each other.

An internal zone and an external zone are defined on the firewall during installation. The external zone is the Internet zone; it is the only zone that communicates directly with the outside world, and it cannot be removed.

Note: Zone objects were referred to as burb objects in version 7.x firewalls. If you are looking for your burb objects to edit, you can find them beneath the **Zones** node in the tree on the **Rule Objects** tab of the **Policy** icon.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Network Objects** node.

4) Double-click the **Zones** node. The **Zones** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Select a firewall and the zone options for the firewall.

6) Repeat step 5 for each firewall in the zone.

7) Click **OK**.

Result

The new zone object is added to the **Zones** node and can be used in a rule.

Create a group of zone objects

You can define a group of zone objects that will be managed simultaneously.

The purpose of a group is object-specific; however, the act of creating groups is the same. Two or more related objects are associated under an aggregated object name to simplify management of multiple objects.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Network Objects** node.

4) Double-click the **Zone Groups** subnode. The **Zone Groups** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Select the zones to include in the group.

6) Click **OK**.

Result

The new zone group is added to the **Zone Groups** node, and can be used in a rule.

Create a netmap object

You can create a netmap object to map multiple IP addresses and subnets to alternate addresses without creating numerous access control 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.

When you create a netmap object, it appears in three different locations: beneath the **Netmaps** node under the **Network** Objects node in the **Rule Objects** tree of the **Policy** icon and in the list of objects in the **Sources** list and the **Destination** list in the **Access Control Rule Editor** window. You can select the object in the **Sources** list or in the **Destinations** list of the **Access Control Rule Editor** window or you can select it in the **Rule Objects** tree and drag it to the **Sources** or **Destination** list.

In an access control rule, you can use a netmap object in the one of two ways:

- Source — Outgoing traffic will be translated to a different originating address.
- Destination — Incoming traffic will be redirected to specific addresses.

Note: You can also create netmaps dynamically for Network Address Translation (NAT) and redirect access control rules by selecting **Custom Netmaps** from within the **NAT** and **Redirect** fields on the Access Control Rule Editor window. However, these netmaps apply only to the current access control rule and cannot be reused.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the Rule Objects tab.

3) Expand the **Network Objects** node.

4) Double-click the **Netmaps** node. The **Netmap** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description for the netmap.

6) Click **Add**. The **Netmap** Member window appears.

7) Add original and mapped hosts and networks as needed.

8) Click **OK**. The mapped hosts and networks are added to the **Members** table as a new member.

9) Repeat steps 6-8 for each member you want to add to the netmap.

10) Click **OK**.

Result

The new netmap object is added to the **Netmaps** node, and can be used in a rule.

Use a netmap object in an access control rule

By creating and configuring netmap objects, you can use and reuse the same mappings in different access control rules.

Although you can configure netmaps dynamically from within the **Access Control Rule Editor** window (for NAT or Redirect settings), netmap objects are much easier to manage.

> **Note:** This procedure assumes that you have already created netmap objects.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed. If you have a mixture of 7.x and 8.0.0 or later firewalls that are registered to the Control Center, there will be two tabs on this page. Go to the next step.

   or

   If you have only version 8.0.0 or later firewalls, there are no tabs. The **Access Control Rules** page is displayed in the work area. Skip to Step 4.

3) Click the tab for the firewall version for which you want to create the rule. The **Access Control Rules** page is displayed in the work area.

4) In the toolbar, click **Add** to add a new access control rule. The **Access Control Rule Editor** window is displayed.

5) Select one or more firewalls and one or more services (for version 7.x firewall access control rules) or one or more applications, capabilities, and ports (for version 8.0.0 or later firewall access control rules).

6) Select the netmap if you are using NAT.
   - In the **Sources** list, select the netmap
   - You can drag a netmap object from the **Rule Objects** tree to the **Sources** list

7) Select the netmap if you are using redirection.
   - In the **Destinations** list, select the netmap
   - You can drag a netmap object from the **Rule Objects** tree to the **Destinations** list

8) Continue to configure the access control rule and click **OK** when you have finished.

Related tasks

Access control rule management on page 301

Create a group of network objects

You can define a group of network objects that will be simultaneously managed.

The purpose of a group is object-specific; however, the act of creating groups is the same. Two or more related objects are associated under an aggregated object name to simplify management of multiple objects.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Network Objects** node.
4) Double-click the **Net Groups** node. The **Net Group** window is displayed.

   Tip: For option descriptions, press **F1**.
5) Specify the network objects that you want to include in the group.
6) Click **OK**.

Result

The new **Net Group** object is added to the **Net Groups** node and can be used when you define a new rule.

Import network objects

You can import network objects from a file.

The following types of network objects can be imported:

- IP addresses
- Host names for host objects
- Networks
- Address ranges

To create a valid file to use with this wizard, the following prerequisites must be met:

- The file must be in either .txt or .csv (comma-delimited) format.
- You can mix object types in one file. However, each object type must consist of the following format:

Table 9: Imported file formats

Format type	Format	Description
.txt	[Address] [Name] #[Description]	where the address and name parameters are required and the # and description parameters are optional

Format type	Format	Description
.csv	[Address],[Name],[Description]	where the address and name parameters are required and the last comma (,) and the description parameters are optional

- The network object should also include the mask (for example, 1.1.1.1/24).
- The address range object should include the start address and the end address, separated by a hyphen (-) (for example, 1.1.1.1-2.2.2.2).

If there are any errors in your imported file, a message will be displayed and you can view your errors. For more about this, see the wizard steps that follow.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left corner of this window, click the **Rule Objects** tab.

3) Expand the **Network Objects** node.

4) Double-click the **Import Network Objects** node. The **Import Network Objects Wizard** is displayed.

   Tip: For option descriptions, press **F1**.

5) Click **Load File**, then navigate to the file you want to open.

6) Click **Open**. The contents of this file are displayed on the first page of the wizard.

7) Click **Next**. Network objects in the file are listed in the table.

   If there are any errors in the imported file, each row that contains an error is selected and a message is displayed at the bottom of this page, along with a **View Errors** button.

8) Click **Finish**.

Result

The network objects are added to the appropriate nodes and can be used in a rule.

Related tasks
Troubleshoot import network objects errors on page 70

Troubleshoot import network objects errors

You can view and correct errors when importing network objects.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left corner of this window, click the **Rule Objects** tab.
3) Expand the **Network Objects** node.
4) Double-click the **Import Network Objects** node. The **Import Network Objects Wizard** is displayed.
5) Click **View Errors.** The **Import Errors** window appears.
6) Click **x** to close this window.
7) Click in the field in the table that contains the error. Edit the value so that it is correct for the type of object in this row. Note that these changes will not be propagated back to the file itself.
8) Repeat Step 3 for each row that contains an error.
9) When you have completed your edits, click **Finish**.

Result

The values are checked again for validity and are imported if they are correct.

CHAPTER 8

Applications

Contents

Applications are objects that are used to classify network connections based on their functionality, rather than their attributes, such as protocols or ports.

About application objects

Application objects in access control rules to determine whether a connection is allowed or denied.

Note: Application objects are available only for firewall version 8.0.0 or later.

Applications are dynamically created, based on ongoing research. By default, Control Center Management server is configured to periodically download application signature updates to make sure that the applications database contains the latest data that can then be pushed down to its managed firewalls.

You can also create your own, custom applications based on existing applications with different port configurations. And you can group together applications to form application group objects that can be used in access control rules.

There are also tools to assist with refining your list of applications when you are working in the selection process because this list can be very long.

Related concepts

Custom applications on page 72
Application groups on page 74
Category filters on page 75

Related tasks

Search for applications by category and risk on page 77

Use of application objects in access control rules

Use access control rules to determine the applications that are allowed and denied.

You can associate applications with an access control rule by selecting any of the following objects:

- **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

Note: You can select application categories only if the access control rule action is deny or drop. Application categories cannot be selected for allow access control rules.

Custom applications

Custom applications are user-defined applications that are based on existing applications (parent applications) whose ports can be modified by the user.

When to use custom applications

Create custom applications in the **Custom Application** window when you need to allow or deny an application that is not included in the application database.

The port type of the custom application is dependent on the properties of the selected parent application. For example, if you select HTTP as your parent application, you can specify only TCP or SSL ports because HTTP is a TCP protocol that can also use SSL.

Create a custom application

Creating a new custom application object.

Steps

1) Access the **Custom Applications** window.
   From the **Rule Objects** tab:
   a) In the navigation bar, select **Policy**.
   b) In the lower left area of the window, click the **Rule Objects** tab.
   c) Expand the **Application Objects** node.

d) Double-click **Custom Applications**. The **Custom Application** window is displayed.

   From the **Access Control Rule Editor** window:

a) In the navigation bar, select **Policy**.

b) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

c) Make sure that you are working with firewall version 8.0.0 or later access control rules.

d) Double-click an access control rule (not a group, just a single rule). The **Access Control Rule Editor** window is displayed.

e) In the **Applications** area, click **Add**. Then select **Custom Application**. The **Custom Application** window is displayed.

   Tip: For option descriptions, press **F1**.

2) In the **Custom Application** window, specify a unique name for this custom application.

3) Specify whether this custom application is a privileged object.

4) [Optional] Specify a description for this object.

5) In the **Parent application** area, if you select **TCP / UDP** or **HTTP**, specify the respective ports and click **OK**.

   or If you want to base this custom application on a different parent application (that is, other than **TCP / UDP** or **HTTP**), select **Other** and continue to the next step.

6) This next step is about selecting the one parent application on which this custom application will be based. Because the list of parent applications can be long, you can use one of the following methods to filter this list:

   - Select one or more risks in the **Filter applications by risk** area.
   - Select one or more categories in the **Filter applications by category** list.
   - Specify one or more characters in the **Select parent application** field and press **Enter**.

7) Select the application in the table and edit the port fields as needed.

8) Click **OK**.

Result

The new custom application object is created.

Application groups

An *application group* is a set of applications. You can create and maintain application groups in the **Application Group** window.

Types of application groups

There are two different types of application groups.

- One that can be used in any type of access control rule
- One that can only be used in allow access control rules

For the allow rules, you can restrict individual categories that will be enabled for the selected applications.

Create an application group

Creating an application group object.

Steps

1) Access the **Custom Applications** window:

   From the **Rule Objects** tab:

   a) In the navigation bar, select **Policy**.

   b) In the lower left area of the window, click the **Rule Objects** tab.

   c) Expand the **Application Objects** node.

   d) Double-click **Custom Applications**. The **Custom Application** window is displayed.

   From the **Access Control Rule Editor** window:

   a) In the navigation bar, select **Policy**.

   b) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

   c) Make sure that you are working with firewall version 8.0.0 or later access control rules.

   d) Double-click an access control rule (not a group, just a single rule). The **Access Control Rule Editor** window is displayed.

   e) In the Applications area, click **Add**. Then select **Custom Application**. The **Custom Application** window is displayed.

2) In the **Application Group** window, specify a unique name for this application group.

3) Specify whether this application group is a privileged object.

4) [Optional] Specify a description for this object.

5) Because the list of available applications can be lengthy, you can use various methods to filter this list:

- Select one or more risks in the **Filter applications by risk** area.
- Select one or more categories in the **Filter applications by category** list.
- Specify one or more characters in the **Available** field and press **Enter**.

6) Move the targeted applications from the **Available** list to the **Selected** list. You can do this in several different ways:

- *One application* — Select an individual application and click the right arrow.
- *Multiple applications* — Press **Ctrl** and select each random application until all of them are selected. Then click the right arrow to move them to the **Selected** list.

7) Specify the rule action that this application group will be used for. If you select the **Allow, deny, or drop** option, this application group can be used in any access control rule. Skip to Step 8.

   If you select **Allow only**, you can use this application group only in allow access control rules. However, you can also have more flexibility in disabling certain optional capabilities with this selection?that is, if the application has more than one optional capability. Go to the next step.

8) In the **Optional capabilities** field, select the checkbox of any optional capability to disable for this application. (When you select the checkbox, it is deselected and is thus, disabled.)

   For example, select xyz as your application and move it from the **Available** list to the **Selected** list. There are several different capabilities for this application that you will see in the **Optional capabilities** list, including **File Sharing** (optional) and **Instant Messaging** (required). You want to deny file sharing only and allow the other capabilities. You can do this only if the **Allow only** value is selected for the **Rule action** field. You would select the **File Sharing** checkbox to disable it. Note that the Instant Messaging capability is not available to be edited because it is a required capability, regardless of the rule action selection.

9) When you have finished selecting applications and editing optional capabilities, click **OK**.

Result

The application group object is created.

Category filters

Category filters are dynamic groups of applications that change when updates are downloaded to the application database that resides on the firewall. View category filter information in the **Category Filter** window.

When to use category filters

Use category filters to block all the applications that use a specific category. Category filters can be used only in deny or drop access control rules.

Category filters are displayed in the **Applications** list on the **Access Control Rule Editor** window. The category filter object name includes a less than symbol (<) at the beginning of the name and a greater than symbol (>) at the end of the name.

View category filter information

View information about category filters.

This includes information about the applications that have been completely or partially blocked by this category filter.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Double-click an existing rule or click **Add** to add a new one. The **Access Control Rule Editor** window is displayed.

4) In the **Applications** area, scroll through the list of applications until you find a category filter or you can type **<** and click **Find** to display all the category filters. (Category filter names are surrounded with greater than [<] and less than [>] symbols.)

5) Double-click the category filter. The **Category Filter** window is displayed.

6) [Optional] In the **Category Filter** window, you can filter the list of completely blocked applications by specifying a few characters in the **Completely blocked applications** field and pressing **Enter**. Only those applications that match the characters that you specified are displayed.

   To remove the filter, click **x**.

7) [Optional] To view information about one of the applications in the **Completely blocked applications** list or in the **Partially blocked applications** list, double-click it. The **Application** window is displayed. View the information and click **Close**. You are back at the **Category Filter** window.

8) [Optional] You can also filter the list of partially blocked applications by specifying a few characters in the **Partially blocked applications** field and pressing **Enter**. Only those applications that match the characters that you specified are displayed.

9) When you have finished with this window, click **Close**.

View information about applications

View application information, including the categories of this application, additional information about the application, and a list of rules in which this application is currently being used.

Steps

1) Access the **Application** window.

   From the **Rule Objects** tab:

   a) In the navigation bar, select **Policy**.

   b) In the lower left area of the window, click the **Rule Objects** tab.

c) Expand the **Application Objects** node.

d) Double-click **Application Groups**. The **Application Group** window is displayed.

   From the **Access Control Rule Editor** window:

e) In the navigation bar, select **Policy**.

f) In the lower left area of the window, click the **Rule Objects** tab.

g) Expand the **Application Objects** node.

h) Double-click **Application Groups**. The **Application Group** window is displayed.

i) In either the **Available** list or the **Selected** list, right-click an application and select **View Application**. The **Application** window is displayed.

2) View the information on this window and click links as needed.

   Tip: For option descriptions, press **F1**.

3) Click **Close** to close the window.

Search for applications by category and risk

Use **Search Applications** window to filter applications by category and risk.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Double-click an existing rule or click **Add** to add a new one. The **Access Control Rule Editor** window is displayed.

4) In the **Applications** area, click **Advanced search**. The **Search Applications** window is displayed.

5) Configure the information on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save the changes.

CHAPTER 9

Services

Contents

Create service objects that describe the type of traffic that will be recognized by the firewall.

About services

A *service* is a description of a network communications protocol. Computers can send information packets to each other by agreeing on a protocol and, for TCP and UDP, a port.

Protocol and port numbers have well-established meanings; for example, IP protocol 89 is used for Open Shortest Path First (OSPF) routing traffic, and TCP (protocol 6) port number 23 is used for the Telnet remote logon application. Control Center service objects are accustomed to the type of traffic that should be matched by an access control rule. Occasionally, they are also used to specify a TCP or UDP port number that a firewall service (for example, a content inspection agent or remote authorization agent) should use to communicate with a remote computer.

By default, proxy services, filter services, and server services are disabled. If you use a proxy, filter, or server service in an enabled access control rule, the firewall automatically enables that service in the corresponding source zone or zones. When all the access control rules that are using a particular service are disabled or deleted, the service is automatically disabled.

Supported services categories

The security firewalls support several categories of services.

- **Proxy services** — Network services that are associated with a proxy agent that is running on the firewall. The proxy agent controls communication between clients on one side of the firewall and servers on the other side. The user's client program communicates with the proxy agent instead of communicating directly with the server. The proxy agent evaluates requests from the client and decides whether to permit or deny those requests, based on your security policy. If a request is approved, the proxy agent forwards the client's requests to the server and forwards the server's responses back to the client. The proxy agent is application-aware. For example, it understands the application layer protocol and can interpret its commands. Proxy agents are used to create proxy services. Proxy services may be TCP-based or UDP-based. Many are defined by default for such TCP-based services as HTTP, FTP, and Telnet and for such UDP protocols as SNMP and NTP. Use the Proxy Service window to create additional proxy services.
- **Filter services** — Each service is a network service that is associated with a filter agent running on the firewall. Filter agents provide another method for clients and servers to communicate. The filter agent inspects and passes traffic at the network layer or the transport layer.

- **Server services** — A server service is a network service that is associated with a server agent, or *daemon*, running on the firewall. Server services are created during initial configuration of the firewall. They include services that are used for the following purposes:
  - Management of the firewall (for example, Admin Console)
  - Access to a networked service (for example, SNMP Agent)
  - Routing services (for example, gated or routed)
  - VPN connections (for example, ISAKMP server)
  - Firewall-specific functions (for example, cluster registration server)

  Basic properties that are associated with these services can be modified; however, additional server services cannot be created.
- **Service Groups** — A *service group* represents a collection of network services that are defined on the firewall.

Agents and services in your policy

When you are planning your security policy, study the agents and the default services to determine those that you will need and the values to assign them.

Consider the following:

- Decide the type of inspection that is needed for each allowed service. Proxy agents inspect traffic at the application layer. Filter agents tend to inspect traffic at the transport layer.
- When possible, use an application-aware or protocol-aware proxy agent instead of a generic proxy agent.
- Consider the way that traffic will travel from one zone to another. Make sure that the appropriate routing is in place and that you know the connection types that are needed (transparent, non-transparent, or both).
- Review the server services to determine your policy requirements, and those servers that need modification. Some servers have advanced properties, such as the ability to add extended authentication to the ISAKMP server or to modify the single sign-on (SSO) server's banners.

Note: There is a security risk involved with using non-application aware services. The firewall has greater control over traffic that is managed by proxies because it can manipulate independent proxy connections on each side of the firewall.

About proxy services

A proxy agent is a program that controls communication between clients on one side of a firewall and servers on the other side. The client and server do not communicate directly. Instead, the client and server both "talk" to the proxy agent that is running on the firewall, which forwards the data back and forth.

How the firewall improves proxy connections

The firewall increases the security of a proxy connection by receiving each packet, rebuilding it, and then sending it on its way.

The traffic’s source, or initiator, sends out a request that is routed through the firewall. It inspects the packet, making sure that the security policy allows the request. Next, the firewall checks whether any advanced checks, such as IPS or Application Defense inspection, are required. After the firewall finishes handling the request, it rebuilds the packet and sends it to its destination. The firewall also keeps track of the requests that were allowed and permits the appropriate responses.

The proxy agents are used to create proxy services. By default, proxy services are disabled. When you use a proxy service in an enabled rule, the firewall automatically enables that service in the corresponding source zone or zones.

Add a proxy service

You can add a proxy service to the **Proxy Services** node.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Services** node.

4) Double-click the **Proxy Services** node. The **Proxy Service** window appears.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description.

6) Select the type of traffic that will use the service.

7) Complete the remaining fields.

8) Click **OK**.

Result

The new service is added to the **Proxy Services** node and can be used in rules.

About filter services

A filter service is a network service that is associated with a filter agent running on the firewall. Filter agents provide another method for clients and servers to communicate. The filter agent inspects and passes traffic at the network layer or the transport layer.

Types of filter agents

Several types of filter agents are provided.

- **FTP Packet Filter** — File Transfer Protocol (FTP) is a file transfer protocol that is defined by specified port numbers. This agent supports both active and passive FTP by monitoring the control connection and dynamically opening a port for the data connection. To allow FTP over IPv6, you must use this agent. The FTP proxy agent does not support IPv6.

- **Generic Filter** — This is a network service that is associated with a proxy agent that is running on the firewall. The proxy agent controls communication between clients on one side of the firewall and servers on the other side. Proxy services may be TCP-based or UDP-based.
- **ICMP Filter** — Internet Control Message Protocol (ICMP) is a network layer protocol that supports packets that contain error, control, and informational messages. A message type and code further qualify the service.
- **Protocol Filter** — This is a network layer protocol that is defined by a protocol number.

Filter agents are used to create filter services. A wide range of filter services is defined by default. Use the **Filter Service** window to create additional filter services.

Create a filter service

You can add a filter service.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Services** node.

4) Double-click the **Filter Services** node. The **Filter Service** window appears.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description.

6) Complete the remaining fields.

7) Click **OK**.

Result

The new service is added to the **Filter Services** node and can be used in rules.

Configure service groups

You can create a group of related services.

The purpose of a group is specific to the type of service. However, the procedure to create groups is the same. Two or more related objects are associated under an aggregated object name to simplify the management of multiple service objects.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Services** node.

4) Double-click the **Service Groups** node. The **Service Group** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description for the service group.

6) Select the type of services the group will include.

7) Select the specific services the group will include.

8) Click **OK**.

Result

The new group is added to the **Service Groups** node, and can be used in rules.

CHAPTER 10

Application Defenses

Contents

Use Application Defenses to configure advanced properties for access control rules. You can refine access control rules for specific applications that use proxies and filter agents. You can also configure key services such as virus protection, spyware protection, SSL decryption, and web services management.

Configure Citrix Application Defenses

Create and maintain Citrix® Application Defense objects.

You can use the Citrix Application Defense to configure advanced properties for the Citrix ICA (Independent Computing Architecture) proxy. This proxy allows users to locate and connect to a Citrix server farm within a private address space. By configuring a Citrix Application Defense, you can control access to resources by enabling filtering of certain types of Citrix ICA application and communication channels (for example, drive mapping, clipboard operations, and printers).

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **Citrix** node. The **Citrix Application Defense** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure FTP Application Defenses

Create and maintain FTP Application Defense objects in the **FTP Application Defense** window.

An FTP Application Defense configures advanced properties for FTP. Such properties include the types of FTP commands allowed and the parameters to use in scanning files transferred by using FTP.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **FTP** node. The **FTP Application Defense** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Generic Application Defenses

Configure advanced connection properties for filter agents and whether stateful packet inspection is used in the **Generic Application Defense** window.

Note: This Application Defense is available only for firewall version 8.0.0 or later.

There are two default Generic Application Defense objects that are predefined for your use:

- **Connection settings** — This object provides connection settings (timeouts).
- **Minimal proxy** — This object is configured to force sessions through a firewall proxy without any additional enforcements.

Related tasks

Configure Generic Application Defenses on page 87

Configure Generic Application Defenses

Create and maintain Generic Application Defense objects.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **Generic** node. The **Generic Application Defense** window is displayed.

5) On the **General** tab, specify the proxy settings.

   Tip: For option descriptions, press **F1**.

6) On the **Stateful Inspection** tab, specify the message types and track individual filter sessions for TCP, UDP, and ICMP filters. Only those packets that are valid for a new session or for a portion of an existing session are sent on to their final destination.

7) On the **IPv6 Header Filtering** tab, configure the IPv6 headers for ICMP filters that you want to allow.

8) On the **Other IP Filter Settings** tab, specify the request rate and audit parameters.

9) Click **OK** to save this object.

Proxy connection settings for a Generic Application Defense

On the firewall, FTP, HTTP, Oracle, and Telnet proxy agents can be configured to be transparent, non-transparent, or both.

For transparent connections, the Client application is unaware of the firewall. The firewall is implicitly included in the path, based on routing. The user appears to connect directly to the network's server without first connecting to the firewall.

For non-transparent connections, the Client application is aware of the firewall and explicitly connects to the firewall. The connection type is determined on the client machine, either by browser settings or by the user inputting the IP address of the firewall.

Proxy services can be configured to allow only transparent connections, only non-transparent connections, or both, depending on the **Allowed connection types** value that is specified in the **Proxy Service** window.

To override these settings, use the **Proxy Connection Settings** window.

Configure proxy connection settings for a Generic Application Defense

Configure proxy connection settings and override the settings specified in the **Proxy Service** window.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **Generic** node. The **Generic Application Defense** window is displayed.

5) Make sure that the **General** tab is displayed.

6) In the Advanced area, click **Connection settings**. The **Proxy Connection Settings** window is displayed.

7) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

8) Click **OK** to save this object.

Configure H.323 Application Defenses

Create and maintain H.323 Application Defenses.

H.323 is an International Telecommunication Union (ITU) standard that specifies how multimedia terminals, equipment, and services communicate over networks that do not provide a guaranteed quality of service (such as the Internet). H.323 allows users to participate in the same video conference even if they are using different video conferencing applications.

Use the **H323 Application Defense** window to make sure that permissions are checked and that only specified audio and video codecs are allowed. *Codecs* define the format for transmitting audio and video information.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **H.323** node. The **H323 Application Defense** window is displayed.

5) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure HTTP Application Defenses

Create and maintain HTTP Application Defenses in the **HTTP Application Defense** window.

An HTTP Application Defense specifies advanced properties for HTTP. These properties include: connection parameters, URL control properties that include URL normalization (for firewall version 8.0.0 or later), header filtering for HTTP requests and replies, content filtering using SmartFilter, and resource scanning for MIME, viruses, and spyware.

For encrypted traffic, the only settings that can be enforced are for SmartFilter (on the **Content Scanning** tab) and for the settings on the **Connection** tab. For firewall version 8.0.0 or later, additional enforcements can be used by initially decrypting the traffic in an SSL rule configuration. For firewall version 7.x, use the **HTTPS Application Defense** window for the additional enforcements.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **HTTP** node. The **HTTP Application Defense** window is displayed.

5) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure HTTPS Application Defenses

Create and maintain HTTPS Application Defenses.

An HTTPS Application Defense specifies advanced properties for HTTPS proxy rules. These properties include connection parameters, SSL decryption, URL control properties, header filtering for HTTP requests and replies, content filtering by using SmartFilter, and resource scanning for MIME, viruses, and spyware.

The **HTTPS Application Defense** window is not available for firewall version 8.0.0 or later. Instead, you must configure an appropriate SSL rule on the **SSL Rule** page to use with the **HTTP Application Defense** window.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **HTTPS** node. The **HTTPS Application Defense** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure IIOP Application Defenses

Create and maintain Internet Inter-ORB Protocol (IIOP) Application Defenses.

An IIOP Application Defense specifies such properties as those controlling bidirectional GIOP, validation of content, and maximum message size.

IIOP is General Inter-ORB Protocol (GIOP) that is operating in a TCP/IP environment. The IIOP proxy provides transparent GIOP access through the firewall that thereby allows Common Object Request Broker Architecture (CORBA) applications to access CORBA resources on configured networks as permitted by the site security policy.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **IIOP** node. The **IIOP Application Defense** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure Mail (Sendmail) Application Defenses

Create and maintain Sendmail Application Defenses.

A Sendmail Application Defense is used in Sendmail rules.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Application Defenses** node.
4) Double-click the **Mail (Sendmail)** node. The **Mail (Sendmail) Application Defense** window is displayed.
5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.
6) Click **OK** to save this object.

Configure Mail (SMTP proxy) Application Defenses

Create and maintain Mail (SMTP proxy) Application Defenses.

The Mail (SMTP Proxy) Application Defense is used to filter mail by using the SMTP proxy rules and is used to conceal your internal mail infrastructure.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Application Defenses** node.
4) Double-click the **Mail (SMTP Proxy)** node. The **Mail (SMTP proxy) Application Defense** window is displayed.
5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure MS SQL Application Defenses

Create and maintain MS SQL Application Defenses in the **MS SQL Application Defense** window.

> **Note:** The MS SQL Application Defense is not currently available. It is reserved for future features.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Application Defenses** node.
4) Double-click the **MS SQL** node. The **MS SQL Application Defense** window is displayed.
5) Configure the fields on this window as needed.

   > **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure Oracle Application Defenses

Create and maintain continuous session monitoring to prevent spoofing and tunneling attacks while sessions are in progress for the SQL proxy in the **Oracle Application Defense** window.

Use this window to indicate whether Oracle® service name checking is enabled and to configure the service names that are allowed access to the SQL server.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Application Defenses** node.
4) Double-click the **Oracle** node. The **Oracle Application Defense** window is displayed.
5) Configure the fields on this window as needed.

   > **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Packet Filter Application Defenses

Packet filter agents are another method for client and servers in different zones to communicate.

They pass traffic at the network layer or the transport layer of the network stack. Filter rules filter incoming packets based on source IP address, destination IP address, and ports.

Similar to proxy rules, filter rules have the option of using network address translation or redirection. Unlike proxy agents, filter agents are not application-aware and cannot enforce traffic based on the application protocol.

TCP, UDP, and ICMP fIlters can actively track individual filter sessions by using stateful inspection. This ensures that only those packets that are valid for a new session or a portion of an existing session are sent on to the final destination.

Note: Packet filter application defense objects are supported only on 7.x firewalls.

Filter services are useful in the following situations:

- Traffic that is a protocol other than TCP or UDP, such as AH, ESP, and GRE.
- TCP/UDP protocols where you need a wide port range or maximum performance with minimal security.
- Proprietary traffic that has invalid TCP/UDP headers.

Filter processing can be configured to reject the following source address packets:

- Packets with broadcast source addresses
- Packets with source addresses on a loopback network that were received on a non-loopback device

Note: Packets that are rejected for source route information generate a netprobe audit event.

Packet filter agent selection

To use a Packet Filter Application Defense, you must first have configured a service that uses a filter agent.

Next, you must have already applied that service to an access control rule. A filter agent is responsible for handling a service's traffic.

The following filter agents can be used to create services:

- TCP/UDP Packet Filter — Use to create services for the UDP and TCP protocols.
  The TCP/UDP packet filter is the only packet filter agent that has configurable agent properties.
- ICMP Packet Filter — Use to create services for the ICMP protocol.
- FTP Packet Filter — Use to create services for the File Transfer Protocol (FTP) traffic.
  This agent supports active and passive FTP by monitoring the control connections and dynamically opening a port for the data connection.

  To allow FTP over IPv6, you must use this agent. The FTP proxy agent does not currently support IPv6.
- Other Protocol Packet Filter — Use to create services for traffic that is not based on the TCP or UDP protocols. This includes protocols such as AH, ESP, and GRE.

Configure advanced properties for access control rules that use filter agents on the **Packet Filter Application Defense** window.

Related tasks
Configure Packet Filter Application Defenses on page 94

Configure Packet Filter Application Defenses

Create and maintain Packet Filter Application Defense objects.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **Packet Filter** node. The **Packet Filter Application Defense** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure SIP Application Defenses

Create and maintain Session Initiated Protocol (SIP) Application Defenses.

As described in RFC 3261, SIP is "an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences."

The SIP proxy provides transparent Voice over Internet Protocol (VoIP) access through the firewall, allowing users to talk through SIP devices on configured networks according to the site security policy. SIP is used to establish multimedia sessions between endpoints. The SIP proxy transfers the SIP traffic that negotiates the multimedia sessions, as well as the multimedia traffic itself.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **SIP** node. The **SIP Application Defense** window is displayed.

5) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure SNMP Application Defenses

Configure advanced properties for the Simple Network Management Protocol (SNMP) Application Defense.

Such properties include the type of SNMP traffic to allow, the types of requests and events to filter, and for SNMP version 1 traffic, the object identifiers to allow or deny.

SNMP is used to manage and monitor network devices such as routers, servers, switches, hubs, and hosts. It accesses hierarchical databases called management information bases (MIBs) to manage the devices in a network. Entries in the MIB are addressed by a unique object identifier, or OID. An OID is a unique numeric representation of a device in the SNMP network. For an understanding of OIDs, MIBs, and SNMP, review the following RFCs:

- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*
- RFC 1157, *A Simple Network Management Protocol (SNMP)*

For assistance in obtaining OIDs, consult the Internet Assigned Numbers Authority (IANA) website at http://www.iana.org/assignments/enterprise-numbers.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **SNMP** node. The **SNMP Application Defense** window is displayed.

5) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure SOCKS Application Defenses

Create and maintain advanced properties for the SOCKS proxy.

Use SOCKS Application Defenses to determine whether SOCKSv4 is supported, to indicate the types of traffic allowed, and to specify the destination ports of the application server.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **SOCKS** node. The **SOCKS Application Defense** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure SSH Application Defenses

Create and maintain SSH Application Defense objects. SSH Application Defenses allow you to configure advanced properties for SSH proxy rules.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **SSH** node. The **SSH Application Defense** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure T120 Application Defenses

Create and maintain T120 Application Defenses.

Use T120 Application Defenses to make sure permissions are checked to determine whether a connection is allowed and to make sure only specified T.120 services are permitted over that connection.

The T.120 standard produced by the International Telecommunication Union (ITU) is composed of a suite of communication and application protocols for real-time data connections and multimedia conferencing. These protocols are used to support whiteboarding, file transfer, application sharing, and text chat.

The T.120 proxy facilitates the control of T.120 services. It can control the T.120 nodes that are allowed to initiate a connection to other nodes and it can mediate the services that are allowed during a session over an allowed connection between nodes.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Application Defenses** node.
4) Double-click the **T.120** node. The **T120 Application Defense** window is displayed.
5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure Application Defense groups

Create and maintain Application Defense groups.

An Application Defense group consists of one Application Defense for each existing type of Application Defense. Application Defense groups are used in access control rules to specify advanced properties for service groups. One Application Defense group is set as the default and is selected by default when a new access control rule that uses an Application Defense is created. Only Application Defenses that apply to the services that are specified on the access control rule are implemented in the rule.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Application Defenses** node.
4) Double-click the **Group** node. The **Application Defense Groups** window is displayed.
5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

CHAPTER 11

Intrusion Prevention System (IPS)

Contents

Configure IPS response mappings and signature groups.

About IPS inspection

Use the IPS object to configure IPS response mappings and signature groups.

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.

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 may update them occasionally.

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

How IPS inspection strengthens access control rules

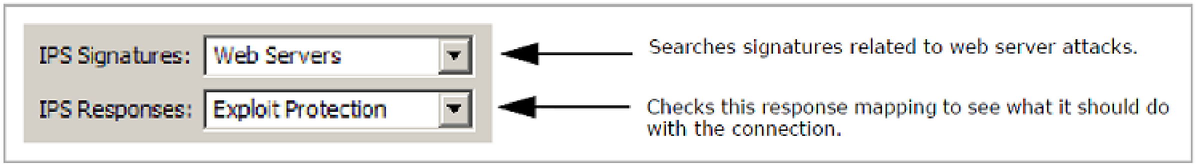
Enable IPS on those access control rules that govern likely targets. Traffic that does not have IPS inspection enabled will not be inspected for network-based attacks.

When you plan your security policy, determine the traffic and systems that are likely to be targets for network-based attacks. IPS is most commonly used to inspect inbound connections because attacks typically come from external, untrusted sources. If an internal server, such as a web server on your DMZ, is compromised, scanning its outbound connections is useful for containing damage and preventing attacks from spreading to other systems.

Tip: 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 Response** window.

The following figure is an example of an access control rule with IPS inspection enabled. When HTTP traffic that is destined for the vulnerable_web_server reaches the firewall, the firewall checks that traffic against signatures in the “Web Servers” signature group. When the pattern of the traffic matches an attack, the firewall checks the “Exploit Protection” response mapping to determine the way that it should respond to the class type that is associated with that attack.

Figure 4: IPS on a rule



IPS Signatures: Web Servers

IPS Responses: Exploit Protection

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

IPS inspection is controlled on a per-rule basis. If you configure the inspection of all traffic by using IPS signatures, the performance of your firewalls can be greatly reduced. However, if you enable IPS inspection only when it is needed, the resources of your firewalls can focus 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.

Related information

How access control rules work on page 297

About IPS response mappings

A response mapping contains a list of class types, the threat level of each type, and the response setting for each type.

Each class type refers to a set of known network-based attacks that are defined by the nature and severity of attack (for example, backdoor activity, root-level exploit, worms, and viruses).

Class types with an IPS classification detect confirmed attacks that are also considered to be dangerous. Class types with an IDS classification detect suspected attacks or traffic that is considered less dangerous, such as probe or discovery activity. Class types with a Policy classification identify traffic based on organizational security practices.

The response mapping objects that you create and manage in the **IPS Response Mapping** window can be selected in the **Access Control Rules** window to indicate the way that the firewall will respond when an attack is detected.

Related tasks

Configure IPS Response Mappings on page 101

Configure IPS Response Mappings

Create and maintain IPS Response Mappings.

After a response mapping is configured, it can then be selected on the **Access Control Rules** window to indicate the way that the firewall will respond when a related attack is detected.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **IPS** node.
4) Double-click the **Response Mappings** node. The **IPS Response Mapping** window appears.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description for the response mapping.
6) Select a response for each class type.
7) Click **OK**.

About IPS signature groups

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 it might update them occasionally.

Use signatures to detect particular types of network attacks (for example, back-door activity, root user exploit, worms, and viruses). They are contained in signature categories such as BROWSER - IE, DB - MSSQL, and FTP - LOGIN, and those signature categories can be grouped.

You can also add individual signatures to a signature group. This provides finer control when creating a signature group. You can also add policy signatures, which are not included in the default signature categories because they are specific to an organization.

Signature group objects are configured in the **IPS Signature Group** window. You can then select them in the **Access Control Rules** window to focus IPS inspection on relevant attacks.

Related tasks

Configure IPS signature groups on page 102

Configure IPS signature groups

Create and maintain IPS signature groups.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **IPS** node.

4) Double-click the **Signature Groups** node. The **IPS Signature Group** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description for the IPS signature group.

6) Enable and disable signature categories or specific signatures as needed.

7) Click **OK**.

CHAPTER 12

SmartFilter management

Contents

SmartFilter software is a web filtering solution that is designed to manage access to the Internet. Using SmartFilter, you mitigate 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.

About SmartFilter

SmartFilter uses web reputation and categorization, which contains 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 that are categorized as unproductive or non-business related. SmartFilter web filtering is performed on a per-rule basis.

Note: SmartFilter is available only for firewall versions 8.0.0 or later.

To filter web traffic by using SmartFilter, you must perform the following tasks:

1) Choose a management method.
2) Configure a SmartFilter management method.
3) Enable SmartFilter on the appropriate access control rules.

Related concepts
SmartFilter management options on page 104

Related tasks
Configure the firewall SmartFilter policy to be managed by the Control Center on page 108
Enable SmartFilter on an access control rule on page 109

SmartFilter management options

The SmartFilter area in the **Offbox** area of the **Firewall** window (for firewall versions 8.0.0 or later) is used to configure the entity that is going to manage SmartFilter policy on this firewall.

The following management options are available when you use SmartFilter with the firewall:

- **Managing SmartFilter with Control Center and Sidewinder** — Use the Sidewinder Control Center Client application to manage SmartFilter policy. This option provides reduced functionality.
- **Managing SmartFilter with the SmartFilter Administration Console** — Use the SmartFilter Administration Console, which is installed on a standalone computer, to manage SmartFilter policy.

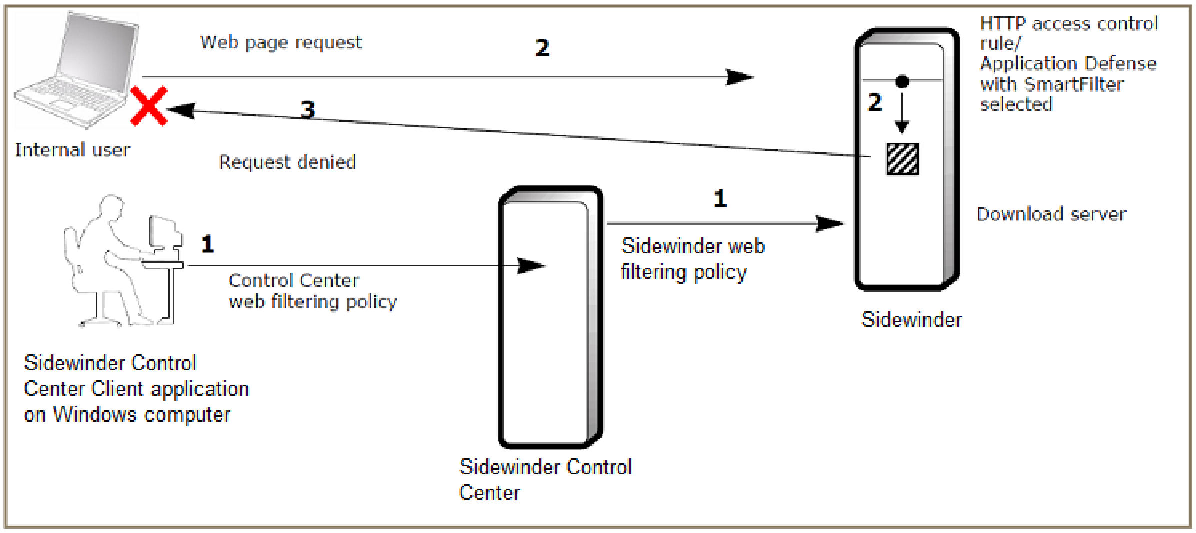
Note: This is a legacy feature and is not actively supported.

Managing SmartFilter with Control Center and Sidewinder

When the Forcepoint Sidewinder Control Center and the Forcepoint Sidewinder are used to manage SmartFilter, basic functionality is available:

- Create filter policy.
- Define custom categories and sites.
- Prefilter HTTP requests by using McAfee Global Threat Intelligence web reputation.
- Require Google and Yahoo! SafeSearch.

Figure 5: Control Center and Sidewinder web filtering process


Web page request
2
3
Internal user
Request denied
HTTP access control rule/
Application Defense with SmartFilter selected
2
1
Download server
Sidewinder web filtering policy
Sidewinder
1
Control Center web filtering policy
Sidewinder Control Center Client application on Windows computer
Sidewinder Control Center

The following actions take place in the figure above.

1) The SmartFilter filtering policy is configured by using the Sidewinder Control Center Client application. This is then applied to the Forcepoint Sidewinder.

2) The firewall checks the user 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 who is making the request.

For more information about configuring the firewall to work with the SmartFilter Administration Console, see the *Forcepoint Sidewinder Product Guide*.

Related tasks
Configure the firewall SmartFilter policy to be managed by the Control Center on page 108

Manage SmartFilter policy on the firewall from the Control Center

To manage SmartFilter in the Control Center Client application, you must perform these tasks.

Configure SmartFilter categories and audit data destinations

Before you enable SmartFilter policy filtering on the Control Center, you must first create **SmartFilter Settings** objects that will be used in the filtering process. Use the **SmartFilter Settings** window to create these objects.

You can add custom sites to the default categories, or you can create custom categories. You can also recategorize existing URLs by providing different URLs according to the acceptable use policy of your organization. For example, if SmartFilter categorized www.example.com as Entertainment, you might recategorize it as Alcohol by creating a custom site.

Note: If a URL that is categorized in the Internet Database is then recategorized by using the **Custom sites** area, the Custom sites categorization takes precedence.

SmartFilter can create an audit entry for each HTTP request that it filters. SmartFilter audits are written to the following log files:

- /var/log/audit.raw — Data can be viewed in the **Firewall Audit** page.
- /var/log/SF.log — Data can be viewed on the **SmartFilter Log Report** page.

Create SmartFilter settings objects

You can configure SmartFilter settings.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Firewalls** node.

3) Double-click the firewall on which you want to configure SmartFilter policy.

4) In the tree, click **Offbox**. The **Offbox** area is displayed.

5) In the **SmartFilter** area, under **Management** source, click Control Center.

6) In the **Settings** field, click **Add**. The **SmartFilter Settings** window is displayed.

   Tip: For option descriptions, click **F1**.

7) In the **Categories** area, add any new categories as needed.

   Tip: To add URLs to existing categories, highlight the category in the **Category Name** list and click **Add** in the **Custom sites** area. The **Custom Site** window is displayed, in which you can specify the URL.

8) [Optional] Create audit entries.

   a) Click the **Audit** tab.

   b) Select **Enable** SmartFilter **auditing**.

   c) For the **Audit destination** field, select the destination to which you want the SmartFilter audits to be sent.

   d) [Conditional] If you had selected **Remote McAfee Web Reporter server** or **Both**, specify the values for the **Report server address** and **Port** fields.

      Note: McAfee Web Reporter is a legacy feature and is not actively supported.

9) Click **OK**.

Result

The **SmartFilter Settings** object that you just created is now the value that is displayed in the **Settings** field.

Add a URL to a SmartFilter category

You can add specific server sites to an existing SmartFilter category.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Expand the **SmartFilter** node.

4) Double-click **Settings**. The **SmartFilter Settings** window appears.

5) Make sure that the **Categories** tab is selected.

6) From the **Category Name** list, select the appropriate category.

7) Under Custom <category name> sites, click **Add**. The **Custom Site** window appears.

   Tip: For option descriptions, press **F1**.

8) Enter the URL for the server site, then click **OK**.

Result

The new site is added to the list of URLs for the selected category on the **SmartFilter Settings** window.

Create a custom category

You can add a new custom category to the SmartFilter categories list.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Expand the **Firewall SmartFilter** node.

4) Double-click **Settings**. The **SmartFilter Settings** window appears.

5) Make sure that the **Categories** tab is selected.

6) Under Categories, click **Add**. The **Custom Category** window appears.

   Tip: For option descriptions, press **F1**.

7) Enter the new category name, then click **OK**.

Result

The new category is inserted alphabetically into the list of categories on the **SmartFilter Settings** window.

Specify destinations for SmartFilter audit data

You can specify where SmartFilter audit data will be saved.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Expand the **Firewall SmartFilter** node.

4) Double-click **Settings**. The **SmartFilter Settings** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Click the **Audit** tab.

6) Select the **Enable SmartFilter auditing** checkbox.

7) Select an audit destination, then click **OK**.

Result

The audit information is added to the **SmartFilter Settings** object.

Configure the firewall SmartFilter policy to be managed by the Control Center

You can configure the Control Center to manage SmartFilter policy from the Control Center Client application.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Firewalls** node.

3) Double-click the firewall on which you want to configure SmartFilter policy.

4) In the tree, click **Offbox**. The **Offbox** area is displayed.

   Tip: For option descriptions, click **F1**.

5) In the **SmartFilter** area, under Management source, select **Control Center**.

6) In the **SmartFilter Settings** field, select the settings object to use.

7) Click **OK**. These settings are saved on the **Firewall** window.

Configure filter policies

You can configure web filtering for categories of URLs based on your organization's acceptable use policy.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Firewall Settings** tab.
3) Expand the **Firewall SmartFilter** node.
4) Double-click **Policies**. The **SmartFilter Policy** window is displayed.

   Tip: For option descriptions, click **F1**.

5) Specify a name and description.
6) Select the **Prefilter sites by using GTI checkbox**.
7) For each category, select a filter action.
8) Click **OK**.

Result

The new filter policy is added to the **Policies** node.

Enable SmartFilter on an access control rule

You can enforce SmartFilter web filtering on an access control rule.

Steps

1) Configure SmartFilter on the appropriate HTTP Application Defense.
   a) In the navigation bar, select **Policy**.
   b) In the lower left area of the window, click the **Rule Objects** tab.
   c) Expand the **Application Defenses** node.
   d) Double-click the **HTTP** node to create a new Application Defense or double-click an existing Application Defense. The **HTTP Application Defense** window is displayed.

      Tip: For option descriptions, click **F1**.

e) Click the **Content Scanning** tab and configure it as appropriate.

- Select the **Enforce SmartFilter** checkbox.
- To deny all HTTP requests that occur when SmartFilter is not available, select **Reject all requests if SmartFilter is unavailable**.
- [Control Center-managed SmartFilter] In the Filter policy list, select the filter policy to apply to the access control rule.

f) Click **OK** to save your changes.

2) Configure an Application Defense group.

a) In the navigation bar, select **Policy**.

b) In the lower left area of the window, click the **Firewall Settings** tab.

c) Expand the **Application Defenses** node.

d) Double-click the **Group** node to create a new Application Defense group or double-click an existing Application Defense group. The **Application Defense Groups** window is displayed.

Tip: For option descriptions, click **F1**.

e) Create a new Application Defense group or modify an existing Application Defense group.

f) In the list of Application Defenses for this group, select the HTTP Application Defense object that you configured in Step 1.

g) Click **OK** to save your changes.

3) [Optional] To enable web filtering for HTTPS connections, perform one of the following tasks:

- 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 that you configured in Step 2.

Note: SmartFilter web filtering is not performed for transparent HTTPS connections by using this method.

4) Modify the appropriate access control rule.

a) In the navigation bar, select **Policy**.

b) Click **Access Control Rules**.

c) [Conditional] If you have both 7.x and 8.x access control rules, click the **8.x Firewall Rules (Application-Based)** tab.

d) Double-click the access control rule to which you want to apply SmartFilter or create a new one by clicking **Add**. The **Access Control Rule Editor** window is displayed.

Note: SmartFilter is applied only to the HTTP-based applications.

e) In the **Application Defense** field, select the Application Defense group that you configured in Step 2.

f) Click **OK** to close the **Access Control Rule Editor** window and save your changes.

Related concepts
Generic Application Defenses on page 86
SSL rule management on page 311

Related tasks
Configure Application Defense groups on page 97
Access control rule management on page 301

View information about SmartFilter database versions

You can view the latest version of the SmartFilter database that is installed on one or more selected firewalls.

Steps

1) Go to **Monitor** > **Reports** > **Firewall Reports** > **Smartfilter Database Version**.

   Tip: For option descriptions, click **F1**.

2) Select the firewalls to poll information from, and click **Request Report**.

Result

Database version information for the selected firewalls is displayed in the **Smartfilter Database Version** report.

Related concepts
Firewall reports on page 414

View SmartFilter log information for one or more firewalls

You can view log information from the SmartFilter database that is installed on one or more selected firewalls.

Steps

1) Go to **Monitor** > **Reports** > **Firewall Reports** > **SmartFilter Log**.

   Tip: For option descriptions, click **F1**.

2) Select the firewalls to poll information from, and click **Request Report**.

Result

Log information for the selected firewalls is displayed in the SmartFilter Log report.

Related concepts
Firewall reports on page 414

Configure SmartFilter database updates for the firewall

There are two different ways to update the SmartFilter database on the firewall with the latest categories and sites from the download server.

Create a schedule for updates

You can configure policy updates to the SmartFilter database at a scheduled time.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Expand the **Third-Party Updates** node.

4) Double click an existing **Third-Party Updates** object, or double-click **Third-Party Updates** to create a new one. The **Third-Party Updates** window appears.

   Tip: For option descriptions, click **F1**.

5) Click **SmartFilter Updates**. The **SmartFilter Updates** tab appears.

6) Make sure the **Enable automated updates** checkbox is selected, and specify a frequency and time.

7) Click **OK**.

Result

SmartFilter updates occur at the scheduled time.

Immediately update the SmartFilter database on one or more selected firewalls

You can immediately perform the database updates.

Steps

1) In the navigation bar, select **Maintenance**.

2) In the left area of the window, double-click **Device Control**. The **Device Control** window opens.

   Tip: For option descriptions, click **F1**.

3) Select the firewalls to update.

4) From the **Control Actions** list, select **Download and install most recent SmartFilter database**.

5) Click **Proceed**. A warning message appears.

6) Click **OK**.

Result

The most recent version of SmartFilter is downloaded and installed on the selected firewalls.

CHAPTER 13

Authentication and firewall users

Contents

Authentication refers to a process that validates a person's identity before he or she is allowed to pass traffic through the firewall.

Authentication services

Depending on the authentication method that is used, a person must provide a user name and a valid password and/or a special passcode or personal identification number (PIN) before he or she can be logged onto a server.

If a user enters an invalid password, passcode, or PIN, the policy will not allow network traffic to pass through.

Types of authentication

Sidewinder authenticates two types of users:

- Administrators connecting *to* the firewall
- Proxy users connecting *through* the firewall

Administrator authentication

This is for administrators who maintain or audit the firewall. Administrators log directly into the firewall.

- The initial administrator account, including user name and password for login authentication to the firewall, is created during startup configuration using the Quick Start Wizard.
- Additional administrator accounts can be created or modified on the **Administrator Accounts** window.
- Administrators can use SSH to access a firewall remotely via a command line interface.

Note: We recommend using a strong authentication method for administrators logging in remotely.

Proxy authentication

This is for network users who are attempting to create a proxy connection from one side of the firewall to the other.

- You can authenticate internal-to-external, external-to-internal, and internal-to-internal connections.
- You can authenticate access for any service through the firewall.
- You can allow access to multiple services with a single successful authentication method by using Passport (also known as single sign-on).
- You can require authentication by selecting an authentication method on the **Access Control Rules** page when you create an access control rule.
- You can configure authentication on a user-by-user basis. Some authenticators allow you to create user groups to identify multiple users with a single name, or to add groups from an external authentication server. You can assign groups to use an authentication method for an access control rule in the **Access Control Rules** page.

Related concepts

Creating and configuring authenticators on page 120

Weak and strong authentication

An authentication method is *weak* or *strong*, depending on the level of security it provides.

- **Weak authentication**

  An example of a weak authentication method is a fixed password, which only requires a user to enter the same password every time the he or she logs on. Even if the user carefully chooses a random password, an attacker can sniff the password as it is transmitted and then masquerade as the user.

  Because your internal network is thought to be trusted, fixed passwords can be adequate for internal-to-external authentication.
- **Strong authentication**

  Strong authentication uses a variety of methods to keep passwords secure. A hardware token, for example, generates a different password each time that it is used.

  Authentication can be strengthened by using multiple factors. For example, the hardware token can require a PIN. The user must authenticate by using something he or she has (the token) and something the he or she knows (the PIN).

  Use strong authentication for external-to-internal proxy connections and for external administration access to the firewall.

Authenticator configuration

When users are trying to make a network connection that matches an access control rule, you can use authenticators to validate their identities.

1) Create and configure an authenticator on the respective authenticator window.

2) Select the authenticator on the **Access Control Rule Firewall Editor** window.

3) Select the authenticator in the access control rule.

4) Apply the firewall changes.

5) During logon, a user that matches the rule is prompted to provide a user name and valid password and 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.

Authentication methods

The supported firewalls use similar, but different, objects to support different configuration options for authentication services and access control rules.

When assigning an authenticator to an access control rule, you have the option of restricting proxy connections to specific external user groups, which are configured in the External Group window, which is accessed from the External Groups node under the Users node in the Policy tree of the Policy icon.

The following authentication methods are available in Control Center:

- **Password** — Standard password authentication requires users to enter the same password each time that they log on.
  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.
- **Passport** — Passport works with a specified authentication method to allow access to multiple services with a single successful authentication to the firewall. Passport also allows authentication for encrypted services and services that do not handle authentication.
  You can configure the firewall to revoke the passport after a specified time period has passed (for example, you can choose to require each user to re-authenticate every two hours). You can require a user to re-authenticate after a specified period of idle time. For example, a user must re-authenticate if the passport has not been accessed for one hour or more. You can also manually revoke a Passport for a specific user or for all users at any time.

  Passports can be granted by using either passive or active mode.

  - *Passive mode* leverages an Active Directory server to monitor user authentication information and users are not prompted for authentication by the firewall. This information is communicated to the firewall by the McAfee Logon Collector. When passive passport is configured, users are not prompted to log on to the firewall.
  - *Active mode* (also known as single sign-on) caches the source IP address of an authenticated user for a specified time. A passport is acquired by successfully logging on to the firewall by using a designated authenticator. Subsequent connection attempts from the same IP address are allowed without prompting for authentication.
- **RADIUS** — The Remote Authentication Dial In User Service (RADIUS) is a client/server protocol described in RFC 2138, 2865, and 2866. RADIUS enables remote access servers to communicate with a central server to authenticate users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it is easier to track use and easier to keep network statistics.
  - You can use RADIUS to provide strong authentication for SOCKS 5, Telnet, FTP, and HTTP sessions through the firewall.
  - You can use RADIUS to authenticate logons and SSH logons to the firewall.

> **Note:** SafeWord RemoteAccess and SafeWord PremierAccess are RADIUS servers that have been certified for full interoperability with the firewall.

- **SafeWord** — The SafeWord family of authentication servers that interoperate with the firewall includes SafeWord RemoteAccess and SafeWord PremierAccess.

  > **Note:** For firewall versions 8.1.0 or later, this form of authentication is not directly supported. However, the RADIUS authenticator can be used with a RADIUS server that supports SafeWord tokens to provide authentication by using those tokens.

  With SafeWord PremierAccess, you can use fixed passwords or passcode authentication for Telnet and FTP sessions through the firewall, and for administrator logon attempts directly to the firewall or through an SSH session. You can authenticate HTTP (Not all tokens support this option.)

  To configure SafeWord RemoteAccess authentication, you must use the RADIUS authenticator.
- **Windows Domain** — If your organization operates a Windows primary domain controller (PDC) or backup domain controller (BDC), you can use it to provide authentication for logon, SOCKS 5, Telnet, FTP, HTTP, and SSH sessions to the firewall. The PDC or BDC can be used to provide password authentication. Make sure that the domain controller does not allow blank or default logons that can be easily guessed by outsiders.
  You can also use transparent browser 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 at https://support.forcepoint.com.

  > **Note:** Transparent browser authentication is also known as NT LAN Management (NTLM) or integrated Windows authentication.
- **LDAP** — Lightweight Directory Access Protocol (LDAP) is a protocol that is used by many different authentication servers. You can use the LDAP authentication servers, listed below, to provide fixed password authentication for SOCKS 5, Telnet, FTP, and HTTP sessions through the firewall. It can also be used to authenticate logons and SSH logons to the firewall.
  You can set up an LDAP directory server that contains users and passwords. Use any valid combination of LDAP attributes and values as an optional filter string to distinguish authorized firewall users. You can also define LDAP user groups, which can be used to dynamically create administrator accounts on the Control Center Management Server. If a user attempts to log on and he or she does not have an administrator account on the Control Center Management Server, but he or she does have an account on the LDAP server and he or she is identified on the LDAP server of this LDAP user group, a Control Center administrator account is created automatically on the Control Center Management Server and the administrator object is added to the Firewall Users tree.

  The following LDAP servers are supported:

  - **Active Directory** — Lightweight Directory Access Protocol (LDAP) server owned by Microsoft
  - **iPlane**t — Lightweight Directory Access Protocol (LDAP) server owned by iPlanet, Inc.
  - **Open LDAP** — OpenLDAP Software is a free, open source implementation of LDAP developed by the OpenLDAP Project
  - **Custom LDAP** — Use Custom LDAP to customize the directory user identifier and directory member identifier, the attributes used in the LDAP server searches.
- **Common Access Card (CAC)** — [Available only for firewall versions 7.0.1.02 or later] Use the CAC authenticator to log on to a firewall by using a U.S. Department of Defense Common Access Card (CAC). You can log on to a firewall by using the Forcepoint Sidewinder Admin Console, Telnet, or SSH. Generate a one-time password on a secure webpage on the firewall and specify that password in the appropriate logon field.

  > **Note:** For more information on configuring and using a CAC authenticator, see the application note about configuring Common Access Card authentication at https://support.forcepoint.com.

Identity validation

You can configure the firewall to validate user access by matching their identities.

A user is a person who uses the networking services that are provided by the firewall. A user group is a logical grouping of one or more users, who are identified by a single (group) name. Users and user groups can be used as matching objects in access control rules and SSL rules.

Note: If a user does not match a rule, he or she is not explicitly denied and might be allowed access because of a subsequent rule.

There are two different ways to validate identities:

- **Passive** — User status information is stored on a Microsoft Active Directory server. The McAfee Logon Collector gathers this information and you configure the passive passport on the firewall to communicate with the McAfee Logon Collector. Users are not prompted for authentication by the firewall when they attempt to log on.
- **Active** — An authenticator is configured on the firewall. The firewall prompts users to provide their log on credentials. You can configure an active passport so that the source IP address of an authenticated user is cached, thus allowing subsequent connection attempts without prompting for authentication.

Note: All the IP addresses that are used in identity validation must be IPv4 addresses.

Passive identity validation

Use the passive passport to allow matching users to connect without prompting them 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.

Active identity validation

Active identity validation requires a user to provide a user name and a 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 perform either of the following tasks:

- 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 any prompt for authentication.
- Select the configured authenticator when you create an access control rule. Depending on the authentication method that is configured, a person must provide a user name and a valid password and/or a special passcode or PIN before being logged on to a server.

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

Active passport use

Active passport can be used in the following scenarios.

- **Authenticator groups** — You can designate a group of authenticator objects that can be used to acquire a passport. If you have configured passport as the authentication method in a rule, any of the selected authenticators can be used to authenticate the connection and to acquire a passport.
- **Web login requirement** — 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 is displayed and the user is redirected to the requested webpage. 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 websites. If the user was redirected to the web logon page, the *Successful Login* browser window contains a link to the requested webpage.

  A heartbeat message periodically tests the HTTPS connection and refreshes the *Successful Login* webpage. If the connection is broken, the active passport is revoked. The active passport can also be revoked in any of the following ways:

  - Click **Stop** on the browser window.
  - Close the browser window.
  - Restart the computer.

  When an active passport is revoked, all 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.

Creating and configuring authenticators

Authenticators validate a person's identity before he or she is allowed to pass traffic through the firewall.

Each authentication type is configured in its own window, which can be accessed from the **Authenticators** node on the tree of the **Rule Objects** tab in the **Policy** icon. Authenticator objects can subsequently be selected on the **Access Control Rules** page to authenticate proxy connections.

The following authenticator objects can be created:

- Password
- iPlanet
- Passport
- Active Directory
- RADIUS
- OpenLDAP
- Safeword
- CustomLDAP

- Windows Domain
- CAC

Authenticating with passwords

Standard password authentication requires a user to specify the same password each time that he or she logs in.

Standard password authentication is typically used for internal-to-external SOCKS 5, Telnet, FTP, and HTTP connections through the firewall, and for administrators logging on to the firewall from the internal (trusted) network.

Create password authenticators

Create and maintain standard password authenticators in the **Password Authenticator** window.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Authenticators** node.

4) Double-click the **Password** node. The **Password Authenticator** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Assign a password authenticator to a firewall

Assign a specific password authenticator to a firewall.

Before you begin

You must have already created the password authenticator object in the **Password Authenticator** window.

Steps

1) Assign the password authenticator to the firewall:
   a) In the navigation bar, select **Policy**.

   b) In the **Policy** tree, expand the **Firewalls** node.

c) Double-click the firewall that you want to assign the password authenticator to. The **Firewall** window is displayed.

d) In the navigation tree, click **Settings** > **Policy**. The **Policy** tab is displayed.

e) In the **Password Authenticator** field, select the authenticator to use.

f) Complete other fields as needed.

Tip: For option descriptions, press **F1**.

g) Click **OK** to save the changes that were made in this window.

2) Assign the password authenticator to the access control rule:

a) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

b) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

c) In the **Authenticator** field, select **Password**.

This value is a placeholder. When the policy is applied, this placeholder is replaced with the authenticator that you have specified in the **Password** field on the **Firewall** window.

d) Complete other fields as needed.

Tip: For option descriptions, press **F1**.

e) Click **OK** to save the changes that were made in this window.

3) Apply the configuration changes that have been made to the firewall by clicking **Apply** in the navigation bar.

Related tasks

Create password authenticators on page 121

Authenticating with Passport

Passport (also known as single sign-on) authentication allows user access to multiple services with a single successful authentication to the firewall. Passport also allows authentication for encrypted services and services that do not handle authentication.

You can configure the firewall to revoke the passport after a specified time period has passed (for example, you can choose to require each user to re-authenticate every two hours). You can require a user to re-authenticate after a specified period of idle time. For example, a user must re-authenticate if the passport has not been accessed for one hour or more. You can also manually revoke a Passport for a specific user or for all users at any time.

The type of passport authentication determines the method that is used to provide the authentication for users.

- *Passive authentication* leverages an Active Directory server to monitor user authentication information and users are not prompted for authentication by the firewall. This information is communicated to the firewall by the McAfee Logon Collector. When passive passport is configured, users are not prompted to log on to the firewall.

- *Active authentication* (also known as single sign-on) caches the source IP address of an authenticated user for a specified time. A passport is acquired by successfully logging on to the firewall by using a designated authenticator. Subsequent connection attempts from the same IP address are allowed without prompting for authentication.

Related tasks

Create passport authenticators on page 123

Assign a passport authenticator to a firewall on page 124

Create passport authenticators

Configure Passport authenticator objects in the **Passport Authenticator** window.

They can then be selected in the **Access Control Rule Editor** window to indicate the single-sign on (SSO) authentication that is used for this access control rule.

You can create multiple passport authenticators in the Control Center Client application. In the Forcepoint Sidewinder Admin Console, you cannot rename the default passport authenticator, nor can you create additional passport authenticators.

To create a passport authenticator:

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Authenticators** node.

4) Double-click **Passport Authenticators**. The **Passport Authenticator** window is displayed.

5) Configure the fields on this window as needed.

    Note: In the table on the **Default** tab, a Safeword authenticator will be displayed. However, Safeword authenticators cannot be used for firewall versions 8.1.0 or later.

    Tip: For option descriptions, press **F1**.

6) Click **OK** to save the changes.

Assign a passport authenticator to a firewall

Assign a specific passport authenticator to a firewall.

Before you begin

You must have already created the passport authenticator object in the **Passport Authenticator** window.

Steps

1) Assign the passport authenticator to the firewall:
   a) In the navigation bar, select **Policy**.

   b) In the **Policy** tree, expand the **Firewalls** node.

   c) Double-click the firewall that you want to assign the passport authenticator to. The **Firewall** window is displayed.

   d) In the navigation tree, click **Settings** > **Policy**. The **Policy** tab is displayed.

   e) In the **Passport Authenticator** field, select the authenticator to use.

   f) Complete other fields as needed.

      Tip: For option descriptions, press **F1**.

   g) Click **OK** to save the changes that were made in this window.

2) Assign the passport authenticator to the access control rule:
   a) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

   b) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

   c) In the **Authenticator** field, select **Passport**.

      This value is a placeholder. When the policy is applied, this placeholder is replaced with the authenticator that you have specified in the **Passport** field on the **Firewall** window.

   d) Complete other fields as needed.

      Tip: For option descriptions, press **F1**.

   e) Click **OK** to save the changes that were made in this window.

3) Apply the configuration changes that have been made to the firewall by clicking **Apply** in the navigation bar.

Result

Note: You can manage cached passport users by using the **Current Passport Users** report. To view this report, select the **Monitor** icon and then click the **Reports** tab. Then select **Firewall Reports** > **Current Passport Users**.

Create RADIUS authenticators

When you use a RADIUS authenticator in an access control rule, you have the option of only allowing users from a specified internal user group.

The Remote Authentication Dial In User Service (RADIUS) is a client/server protocol described in RFC 2138, 2865, and 2866. RADIUS enables remote access servers to communicate with a central server to authenticate users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it is easier to track use and easier to keep network statistics.

If your organization operates a RADIUS server, you can use it to provide strong authentication for SOCKS 5, Telnet, FTP, and HTTP sessions through the firewall. It can also be used to authenticate logons and SSH logons to the firewall. SafeWord® RemoteAccess™ and SafeWord® PremierAccess™ are RADIUS servers that have been certified for full interoperability with the firewall.

Create and maintain your RADIUS authenticator objects in the **RADIUS Authenticator** window.

They can then be selected in the **Access Control Rule Editor** window to indicate the single-sign on (SSO) authentication that is used for this access control rule.

You can create multiple RADIUS authenticators in the Control Center Client application.

To create a RADIUS authenticator:

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Authenticators** node.

4) Double-click **RADIUS Authenticators**. The **RADIUS Authenticator** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save the changes.

Create Safeword authenticators

Create and maintain your SafeWord® authenticators in the **Safeword Authenticator** window.

The SafeWord family of remote authentication servers includes SafeWord® RemoteAccess® and SafeWord® PremierAccess®. With SafeWord PremierAccess, you can use fixed passwords or passcode authentication for Telnet and FTP sessions through the firewall, and for administrator logon attempts directly to the firewall or through an SSH session. You can authenticate HTTP sessions by using either fixed passwords or passcodes without the challenge or response option. (Some tokens do not support this option.)

When you create an access control rule, you can also select the external group or groups that will be required to authenticate when those users attempt to pass traffic that matches that rule.

Note: You cannot use Safeword authenticator objects on firewall versions 8.1.0 or later. They can still be used on firewall versions 7.x and 8.0.0.

To create a Safeword authenticator:

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Authenticators** node.
4) Double-click **Safeword Authenticators**. The **Safeword Authenticator** window is displayed.
5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.
6) Click **OK** to save this object.

Create Windows Domain authenticators

Create and maintain your Windows Domain authenticators in the **Windows Domain Authenticator** window.

A Windows Domain authenticator consists of a list of Windows primary domain controllers (PDC) and backup domain controllers (BDC) that the firewall can query to authenticate users. This authentication method can be used to provide authentication for logon, SOCKS 5, Telnet, FTP, and HTTP, as well as SSH sessions to the firewall. Use this window to specify the prompts and messages that are displayed to users, as well as to determine whether prompted or transparent authentication is to be used. (Transparent browser authentication is also known as NTLM or integrated Windows authentication.)

Authenticators are used in access control rules to require users to authenticate to the specified server before their request is allowed through the firewall. When you use a Windows Domain authenticator in an access control rule, you also have the option of only allowing users from a specified internal user group.

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

To create a Windows Domain authenticator object:

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Authenticators** node.

4) Double-click **Windows Domain Authenticators**. The **Windows Domain Authenticator** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Create iPlanet authenticators

Create and maintain iPlanet Authenticators in the **iPlanet Authenticator** window.

An iPlanet server is an LDAP server owned by iPlanet, Inc.

To create an iPlanet authenticator object:

Note: Create all host objects for authentication servers and external groups before configuring this authenticator. Host objects must have an IP address or they will not appear in the **Host** lists.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Authenticators** node.

4) Double-click **iPlanet Authenticators**. The **iPlanet Authenticator** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Create Active Directory authenticators

Create and maintain your Active Directory authenticators in the **Active Directory Authenticator** window.

Authenticators are used in access control rules to require users to authenticate to the specified server before their request is allowed through the firewall. An Active Directory server is a Lightweight Directory Access Protocol (LDAP) server that is owned by Microsoft.

To create an Active Directory authenticator object:

> **Note:** Create all host objects for authentication servers and external groups before configuring this authenticator. Host objects must have an IP address or they will not appear in the **Host** lists.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Authenticators** node.
4) Double-click **Active Directory Authenticators**. The **Active Directory Authenticator** window is displayed.
5) Configure the fields on this window as needed.

   > **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Create OpenLDAP authenticators

Create and maintain OpenLDAP authenticators in the **OpenLDAP Authenticator** window.

OpenLDAP Software is a free, open source implementation of LDAP developed by the OpenLDAP Project.

To create an OpenLDAP authenticator object:

> **Note:** Create all host objects for authentication servers and external groups before configuring this authenticator. Host objects must have an IP address or they will not appear in the **Host** lists.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Authenticators** node.
4) Double-click **OpenLDAP Authenticators**. The **OpenLDAP Authenticator** window is displayed.

5) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Create custom LDAP authenticators

Create and maintain custom LDAP authenticators in the **Custom LDAP Authenticator** window.

The primary difference between a Custom LDAP Authenticator and the other LDAP-based authenticators is that you can customize the directory user identifier and the directory member identifier.

> **Note:** Create all host objects for authentication servers and external groups before configuring this authenticator. Host objects must have an IP address or they will not appear in the Host lists.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Authenticators** node.

4) Double-click **Custom LDAP Authenticators**. The **Custom LDAP Authenticator** window is displayed.

5) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Create CAC authenticators

CAC authenticators are used in access control rules to require users who are using CACs for authentication to authenticate to the CAC webserver on the firewall before their request is allowed through the firewall.

> **Note:** Create all host objects for authentication servers and external groups before configuring this authenticator. Host objects must have an IP address or they will not appear in the **Host** lists.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Authenticators** node.

4) Double-click **CAC Authenticators**. The **CAC Authenticator** window is displayed.

5) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Result

To assign a specific CAC authenticator to a firewall, use the **Settings** tab of the **Certificates** area of the **Firewall** window. In the **CAC Authenticator** field, select the appropriate authenticator. You must also specify a certificate on this tab to be used by the CAC Webserver on the firewall. When you create access control rules in the **Access Control Rule Editor** window, set the **Authenticator** field value to **CAC**, which is a placeholder. When the policy is applied, that placeholder is replaced with the authenticator that you have specified in the **CAC Authenticator** field.

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

McAfee Logon Collector

McAfee Logon Collector software is a Microsoft® Windows-based distributed collector.

McAfee Logon Collector polls Active Directory domain controllers for user characteristics, and sends this information to security appliances to correlate network traffic with user behavior. McAfee Logon Collector is installed on a separate Windows-based server to communicate with the directory. This solution does not require any modification to the Active Directory or to the Active Directory directory schema and requires no agents.

Manage communication with McAfee Logon Collector

Add, edit, or delete MLC connection setting objects.

To display MLC users, MLC user groups, and MLC distribution lists that you can then select for the **User and User Groups** list on the **Access Control Rule Editor** window, you must have previously established communication with a McAfee Logon Collector server.

Steps

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

1) In the navigation bar, select **Control Center**.

2) Click the **MLC Connection Settings tab**.
The **MLC Connection Settings** page is displayed.

Result

You can perform the following actions on this page by clicking these buttons in the toolbar:

- **Add** — Displays the **MLC Connection Settings Editor** window, where you can create a new McAfee Logon Collector connection settings object.
- **Edit** — Displays the **MLC Connection Settings Editor** window, where you can edit an existing McAfee Logon Collector connection settings object.
- **Delete** — Deletes the selected McAfee Logon Collector connection settings object or objects from the table on this page.

Configure communication with McAfee Logon Collector

Create connection settings objects to save your communication settings with a McAfee Logon Collector on the **MLC Connection Settings Editor** window.

Steps

1) In the navigation bar, select **Control Center**.
2) Click the **MLC Connection Settings** tab. The **MLC Connection Settings** page is displayed.
3) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.
4) Click **OK** to save this object.

Result

This object can now be used to configure passive authentication.

Related tasks
Configure passive authentication on page 131

Configure passive authentication

Configure passive authentication on the Control Center.

The following high-level steps must be used (in this order) so that successful communication between the McAfee Logon Collector and the Control Center can be used to have access to users, groups, and distribution lists on the McAfee Logon Collector server.

Configure the remote certificate

For this passive authentication configuration, the remote certificate is the certificate that is used by the McAfee Logon Collector server.

This procedure takes place on the Control Center Client application. However, you also need to be logged on to the Shared domain.

Use the **Remote Certificates** page to create the remote certificate and to export it locally to your computer.

Steps

1) Do one of the following:
   - If you are logged onto the Shared domain, skip to Step 2.
   - If you have already configured configuration domains, in the **Domain** field, select **Shared** and skip to Step 2.
   - Configure the shared domain. You must create a new domain so that the shared domain becomes available.

   a) In the navigation bar, select **Control Center**.

   b) In the Control Center tree, double-click **Configuration Domains**. The **Configuration Domain** window is displayed.

   c) In the **Name** field, specify a unique name for this configuration domain. The **Description** field is optional.

   d) Click **OK**. A confirmation message is displayed, asking whether you want to continue.

   e) Click **Yes**. A warning message is displayed, advising that other users must be assigned logon privileges and roles for this new domain.

   f) Click **Close**. Another warning message is displayed, indicating that configuration domains are now active and that you must restart the Client application now.

   g) Click **OK**. The Client application closes.

   h) Log on again. In the logon window, type your password and then select **Shared** in the **Domain** field. Then click **Connect**. The Control Center Client application is displayed.

2) You can create a certificate or import an existing one.
   - To import a certificate, complete that task and come back to Step 3.
   - To create a certificate, continue with the steps below.

   a) In the navigation bar, select **Policy**.

   b) Click the **Remote Certificates** tab. The **Remote Certificates** page is displayed.

   c) Click **Add Certificate**. The **Certificate Request Wizard** is displayed.

   d) Select **Create a new certificate** and click **Next**.

   e) In the **Unique Name** field, specify a unique name for the certificate and click **Next**.

f) In the **Common Name** field, enter a common name and select a country in the **Country** field.

g) Complete the rest of the page as needed and click **Next**.

h) [Optional] Specify subject alternative names with IP addresses in either the IPv4 or IPv6 format and click **Next**.

i) Select a public key encryption algorithm and key size and click **Next**.

j) In the **Signature Mechanism** field, select **Self-Signed** and click **Next**.

k) Review your selections.

- If they are acceptable, click **Next**.
- If not, click **Back** until you get to the page that contains the information to change. Make your changes and then click **Next** until you are back at this page.

l) Click **Finish**. The certificate has been successfully imported. You should see it on the **Remote Certificates** page.

3) Export the certificate.

a) Select the certificate that you have just imported on the **Remote Certificates** page and click **Export Certificate**. The **Export Certificate wizard** is displayed.

b) Click **Next**. (Accept the default **Export Certificate** selection.)

c) Click **Browse** and specify the name and a destination of the certificate file and click **Save**. The path and file name are now displayed in the field in the wizard.

d) Click **Next** and **Next** again to confirm the file name and location.

e) Click **Finish**. The certificate has been exported. In the **Status** field on the **Remote Certificates** page, you should now see **Completed: Self Signed**.

Result

Now you are ready to import the remote certificate to the McAfee Logon Collector.

Related tasks
Import the remote certificate to the McAfee Logon Collector server on page 135

Import an existing certificate

Import a pre-existing certificate into the **Certificate** drop-down list on the **MLC Connection Settings Editor** window while you are creating a new MLC Connection Settings object.

Use this procedure only when you have a pre-existing certificates to import into the **Certificate** drop-down list.

Steps

1) In the navigation bar, select **Control Center**.

2) Click the **Logon Collector Connection Settings** tab. The **Logon Collector Connection Settings** window is displayed.

3) Click **Add**. The **MLC Connection Settings Editor** window is displayed.

4) Click **Add** to the right of the **Certificate** field. The **Certificate Request Wizard** is displayed.

5) Select **Import an existing certificate** and click **Next**.

6) In the **Unique Name** field, specify a unique name for the certificate and click **Next**.

7) In the **Import Mechanism** field, accept the default value (**Encrypted File (PKCS12)**) and click **Next**.

8) Configure the certificate location and the password that is required to decrypt the certificate.

   a) Click **Browse** to navigate to the location of the certificate. Double-click it. It is then displayed in the **Certificate** field.

   b) Specify the password in the **Password** and **Confirm Password** fields and click **Next**. A confirmation message is displayed on the last page.

   c) Click **Finish**. The name of the certificate that you just imported is displayed now in the **Certificate** field on the **MLC Connection Settings Editor** window.

9) In the **Common Name** field, enter a common name and select a country in the **Country** field. Complete the rest of the page as needed and click **Next**.

10) [Optional] Specify subject alternative names with IP addresses in either the IPv4 or IPv6 format. Click **Next**.

11) Select a public key encryption algorithm and key size and click **Next**.

12) In the **Signature Mechanism** field, select **Self-Signed** and click **Next**.

13) Review your selections.

    If they are acceptable, click **Next**.

    If not, click **Back** until you get to the page that contains the information to change. Make your changes and then click **Next** until you are back at this page.

14) Click **Finish**. The certificate that you have just created is now displayed in the **Certificate** field of the **MLC Connection Settings Editor** window.

Import the remote certificate to the McAfee Logon Collector server

Use the **Certificates** area of the **Firewall** window to import the remote certificate to the McAfee Logon Collector server.

The remote certificate must be accessible by the McAfee Logon Collector server so that it can import the certificate to the server. In this procedure, you are importing the remote certificate onto the McAfee Logon Collector server.

Steps

1) Log on to the McAfee Logon Collector.

2) In the navigation bar, click **Menu**. Then click **Configuration** > **Trusted CAs.** The **Trusted Authorities** page is displayed.

3) In the lower left corner, click **New Authority**. The **New Trusted Authority** page is displayed.

4) Click **Browse**.

5) Navigate to the destination of the certificate file that you exported and select the certificate file. The path and file name are added to the **Certificate** field.

6) Click **Save**. You should now see the common name of the certificate displayed in the **Trusted Authorities** list.

Result

Now you are ready to configure the McAfee Logon Collector on the Control Center Client application.

Related tasks

Configure the remote certificate on page 132
Configure the McAfee Logon Collector server on the Control Center on page 135

Configure the McAfee Logon Collector server on the Control Center

The McAfee Logon Collector server and the Control Center must be able to communicate with each other so that the Active Directory data can be accessible to the Control Center Client application.

This procedure takes place on the Control Center Client application.

Use the **MLC Connection Settings Editor** window to configure the McAfee Logon Collector server object on the Control Center.

Steps

1) Log on to the Control Center Client application.

2) If you are in the Shared domain, in the **Domain** field, switch to the domain where you will be using the McAfee Logon Collector data. A verification message is displayed. Click **OK**.

   or

   If you do not have configuration domains enabled, skip to the next step.

3) In the navigation bar, select **Control Center**.

4) Click the **MLC Connection Settings** tab. The **MLC Connection Settings** page is displayed.

5) Click **Add**. The **MLC Connection Settings Editor** window is displayed.

6) Configure the MLC connection settings object.

   a) In the **IP address** field, specify the IP address of the McAfee Logon Collector server.

   b) In the Certificate drop-down list, select the Control Center certificate that you imported to the McAfee Logon Collector server. The name of this certificate is the name that you specified in the **Unique Name** field of the **Certificate Request Wizard**.

   c) Click **Retrieve MLC Root Certificate**. Make a note of the name of this certificate. (You will need it on the **Firewall** window later.) If the retrieve is successful, a confirmation message is displayed.

   d) Click **OK**. The certificate from the McAfee Logon Collector server is automatically displayed in the **CA certificate** field.

   e) In the **List of Configuration Domains** list, select one or more domains. Although you can configure only one McAfee Logon Collector server per configuration domain, in this field, you are specifying the configuration domains that can use this McAfee Logon Collector settings object. Therefore, you can select multiple domains.

   f) Click **Test MLC connection**. If the connection is successful, a confirmation message is displayed.

   g) Click **OK** in the confirmation message and click **OK** to save the MLC connection settings object.

Result

The new object is now listed on the MLC Connection Settings page.
You are ready to configure passport authentication for a Passport authenticator object.

Related tasks

Configure the remote certificate on page 132

Configure passive authentication for a Passport authenticator object on page 137

Configure passive authentication for a Passport authenticator object

You can configure passive authentication in a Passport authenticator object by configuring the Passport authenticator object and then applying it to the firewall.

Before you begin

- The McAfee Logon Collector must be installed on the server that contains the Active Directory.
- At least one Forcepoint Sidewinder must be installed.
- At least one instance of an Active Directory with an appropriate domain and domain controller must be available for monitoring by the McAfee Logon Collector.
- All these entities (the McAfee Logon Collector, the Active Directory, and the firewall) must be physically connected and the firewall or firewalls must be registered to the Control Center. This is for communication purposes.
- The McAfee Logon Collector is watching at least one domain and domain logons are being collected from the domain controllers that are configured in the Active Directory. Users belong to at least one domain group.
- A McAfee Logon Collector connection settings object must have been created in the Control Center Client application in the Control Center icon by clicking the **MLC Connection Settings** tab and creating and saving the settings on the **MLC Connection Settings** page.

This procedure is available only for firewall versions 8.0.0 or later.

This procedure takes place on the Control Center Client application.

To configure the Passport Authenticator object to use passive authentication:

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Authenticators** node.

4) Double-click **Passport Authenticators**. The **Passport Authenticator** window is displayed.

5) Make sure that the Default tab is displayed.

6) Select the **Passive (MLC)** checkbox.

7) In the **IP address** field, enter the IP address of the McAfee Logon Collector server or you can click the **Copy MLC settings** button to retrieve the address from the McAfee Logon Collector connection settings object that is located on the **MLC Connection Settings** page.

8) Click **OK** to save the passport authenticator object.

9) Go to the **Firewall** window to complete the Passport authentication portion of passive authentication.

   a) In the **Policy** tree, expand the **Firewalls** node.

b) Double-click the firewall that you are configuring passive authentication for. The **Firewall** window is displayed.

c) In the navigation tree, click **Offbox**. The **Offbox** area is displayed.

d) In the **McAfee Logon Collector (MLC)** area, select the certificate that the firewall will use for its TLS/SSL connections to the McAfee Logon Collector server in the **Certificate** field.

e) In the **CA certificate** field, select the name of the CA certificate that was retrieved on the **MLC Connection Settings Editor** window.

f) In the navigation tree, expand the **Settings** node and click **Policy**. The **Policy** tab of the **Settings** area is displayed.

g) In the **Passport Authenticator** field, select the passport authenticator that you have just edited.

h) Click **OK** to save the firewall changes.

Result

Now you are ready to configure an access control rule that uses the objects from the McAfee Logon Collector server.

Related tasks
Configure communication with McAfee Logon Collector on page 131
Define an access control rule that uses McAfee Logon Collector objects on page 138

Define an access control rule that uses McAfee Logon Collector objects

Now that communication has been established, you are ready to take advantage of selecting MLC users, user groups, and distribution lists from the McAfee Logon Collector for inclusion in your access control rules.

This procedure is available only for firewall versions 8.0.0 or later.

This procedure takes place on the Control Center Client application.

Use the **Identity Browser** to select objects from the McAfee Logon Collector server to use in access control rules.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. If you have a mixture of version 7.x and 8.0.0 or later firewalls that are registered to the Control Center, there will be two tabs on this page. Go to the next step.

   If you have only version 8.0.0 or later firewalls, there are no tabs. The **Access Control Rules** page is displayed in the work area. Skip to Step 4.

3) Click the **8.x Rules (Application-Based)** tab. The **Access Control Rules** page is displayed in the work area.

4) Click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Users and user groups** area, click **Advanced search**. The **Identity Browser** window is displayed.

6) Select one or more MLC users, MLC groups, MLC distribution lists, external groups, firewall users, or firewall groups to add to the **User and user groups** list in the **Access Control Rule Editor** window and click **OK**. Your selections are now displayed in the **Users and user groups** area and they are selected by default.

   Also, these objects will automatically be added beneath their respective nodes in the **Firewall Users** node of the **Rule Objects** tree in the **Policy** icon. They are also available now for use in other firewall version 8.0.0 or later access control rules.

7) Finish configuring this rule and click **OK**.

Result

Now you can apply this change to the firewall. Passive authentication will be established for the MLC users, MLC user groups, and MLC distribution lists that you have selected from the McAfee Logon Collector in the **Identity Browser** window.

Configuring firewall users

The Control Center provides interfaces to manage several types of firewall users.

- **Control Center users** — These are administrative users of the Control Center Client application. Manage these users by using the **Administrators** node of the Control Center tree on the **Control Center icon**.
- **Firewall administrators and users** — These are users, often with administrative privileges, who can authenticate to, or through, the firewall. The privileges and definition requirements vary by firewall type. Manage these users by using the **Firewall Users** node on the **Rule Objects** tab of the **Policy icon**.
- **MLC users** — These are users who are being tracked by the McAfee Logon Collector. You can retrieve these users from the **Identity Browser** window. However, you must have configured communication with the McAfee Logon Collector server to be able to retrieve them.

Differences between types of user accounts and user groups

There are several different types of user accounts and user groups that can be configured on the firewall.

Administrators are people who have accounts on the firewall and who can be granted permission to log directly into the firewall. Most administrators also have a home directory on the firewall. Users are also people who have accounts on the firewall. However, they can be granted permission to access applications or network services only through the firewall. Access is controlled by using access control rules; accounts must be assigned to a group before the accounts can be assigned to an access control rule.

The differences between the types of accounts are described here:

- **Administrators** — An administrator logs directly into the firewall to perform administrative activities. Each administrator account has a home directory and a password stored on the firewall. This is the password information that is used if administrators are required to authenticate using the Password authentication service. Every administrator has a role that defines the level of access.

  - **Admin**— Grants administrator privileges for all areas. This is the default role.
  - **Admin Read Only**— 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.
  - **No admin Privileges**— An administrator with no admin privileges cannot log on to firewall. This role is generally used to temporarily disable an administrator account.

  The administrator accounts can be added to a user group and then can be added to access control rules that require authentication to manage access to applications or services.

- **Users** — A user uses the networking services provided by the firewall. User accounts can be added to user groups and then can be used in access control rules that require authentication to manage access to applications or services.
  - Users for Windows and RADIUS are maintained on their respective remote servers. However, the user groups for Windows and RADIUS must also be maintained on the firewall by using the **User Group** window.
  - Users and user groups for other authentication methods are created and maintained on the respective remote servers.
- **MLC users** — An MLC user can have two different identities—one is the placeholder object that you can create in the MLC User window until the actual user account is configured on the McAfee Logon Collector and the other is the actual user account that has been configured on the McAfee Logon Collector server.

The differences between the types of groups are described here:

- **User groups** — A user group is a logical grouping of one or more users. A user group can be assigned to an access control rule to restrict access to services on and through the firewall. In general, a single user group contains either administrator accounts or user accounts, not both.
- **External groups** — An external group is a logical grouping of one or more users and the user database is stored on a remote authentication server. Authenticators that support external groups are:
  - RADIUS
  - Safeword
  - iPlanet
  - Active Directory
  - OpenLDAP
  - Custom LDAP

  An external group must first be assigned to an authenticator. When that authenticator is used in an access control rule, you can then select that external group.
- **MLC groups** — An MLC group is logical grouping of one or more MLC users and the group database is stored on the Active Directory and monitored by the McAfee Logon Collector server. These groups are used to assign privileges to shared resources.
- **MLC distribution lists** — An MLC distribution list consists of a group of email addresses that are used to send emails to a collection of users. These distribution lists reside on the McAfee Logon Collector server.

Control Center user accounts

The **User Configuration** page allows you to configure administrator, database user, and other special Control Center user accounts.

Table 10: User accounts and privileges

Option	Definition
Root or Super user account	
root password	[Required] Specifies the super user password, who has full access to the Management Server. **Note:** Make sure the password is strong and has printable ASCII characters.
Confirmation	[Required] Re-enter the password for confirmation.
Administrative user account	
Admin user name	[Required] Specifies the supervisor privileges. This is a system administrator account and has access to operating system level privileges.
Password	[Required] Specifies the password to associate with the user that you typed in the **Admin user name** field.
Confirmation	[Required] Re-enter the password for confirmation.
Client account	
Control Center administrator name	[Required] Specifies the logon ID for the Management Server administrator (for example, **ccadmin**). Use this user name whenever you log on to the Management Server in the Client application logon window. By default, the administrator role is automatically assigned to this user, which provides full access, including access to all managed firewalls. You can change these settings after you finish configuring the Management Server.
Password	[Required] Specifies the password to associate with the user that you typed in the **Control Center administrator name** field.
Confirmation	[Required] Re-enter the password for confirmation.
Firewall audit export user account	
Firewall audit export user name	[Required] Specifies the user name, which denotes the Firewall audit export user account on the Management Server. This user account has the privileges to perform configuration backups and export firewall audits to Control Center. The protocol that is used to export the archives to the Management Server is SCP.
Password	[Required] Specifies the password that is assigned to the Firewall audit export user on the Control Center Management Server.
Confirmation	Specifies the password that you specified in the **Password** field.
Database user account	

Option	Definition
Database user name	[Required] Specifies the administrator account that is configured in the Management Server database.
Password	[Required] Specifies the password to associate with the database user account. This account is used to allow the Apache Tomcat server to communicate with the database.
Confirmation	[Required] Re-enter the password for confirmation.

Comparing 5.2.x and 5.3.x users

There are some differences between the 5.2.x users and 5.3.x users. Some of them map to a different user account in 5.3.x and a few have been deprecated.

Table 11: Comparison of user accounts

5.2.x user	5.3.x user	Privileges
root	root	Linux super user
ccadmin	Client account	Client application user with administrator rights to login to the Control Center Server.
mgradmin	Administrative user account	Control Center Server console user to connect to Control Center Server through console or ssh.
ftp	Firewall audit export user account	Control Center Server user used by firewalls to perform firewall configuration backups and firewall audit exports to Control Center via SCP.
dbuser	Database user account	Control Center database user with administrator rights to specific database objects like tables and views.

Deprecated users

These are a few deprecated user names for 5.3.x.

Note: We recommend that you avoid keeping these user names.

- ccserver
- dbadmin
- dcserver
- postgres
- slony
- tomcat

These 5.2.x users do not exist in 5.3.x:

- backup
- dcsadmin

- sso
- secoff

Related concepts

About Control Center administrators on page 489

Configure firewall administrators

You can create and manage firewall administrator accounts on the **Administrator** window.

Each account also has a `/home/username` directory on the firewall. You must assign each firewall administrator to a firewall before he or she can directly log on to that firewall. You must also assign each administrator a role that indicates the types of privileges that he or she has on the selected firewalls. These are the roles you can assign to an administrator:

- **Admin** — An administrator who can view and make any configuration changes.
- **Admin Read Only** — An administrator who can only monitor firewalls, but can't make any configuration changes on the firewall. This user can be created from Control Center and pushed to firewalls and as such has no impact on Control Center.

  Note: Read only admin users on a firewall can't register their firewalls to Control Center. Only **Admin** users can register firewalls to Control Center.

- **No Admin Privileges** — A role that has does not have any administrator privileges.

Access to the firewall is controlled by using access control rules. By default, firewall access is controlled by using the Login Console, Admin Console, and Secure Shell Server rules, which allow access from the anywhere on the internal zone to the firewall internal zone. They also require password authentication. These rules are needed only when an administrator connects directly to the firewall, instead of using the Control Center Client application.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) In the **Rule Objects** tree, expand the **Firewall Users** node.

4) Double-click **Administrators**. The **Administrator** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure firewall users

You can create and maintain user accounts on the **User** window.

To grant or deny a user access to a network resource, first add the user to a user group. Then create an access control rule that specifies the desired authenticator, and then select the appropriate user group in the **Internal User Groups** list.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) In the Rule Objects tree, expand the **Firewall Users** node.

4) Double-click **Users**. The **User** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Related concepts
About Control Center administrators on page 489

Configure firewall user groups

You can create and maintain user groups on the **User Group** window.

A user group is a logical grouping of one or more firewall users, administrators, user groups, MLC users, MLC groups, MLC distribution lists, or external groups. You can nest one or more groups inside of another group. User groups are used in access control rules with Passport, Password, Windows, or RADIUS authenticators, and are listed in the **Internal User Groups** list.

You can lock out users who fail a specified number of consecutive authentication attempts. Lockout settings are managed in the **Settings** area of the **Firewall** window. You can also view a report that lists users who are currently locked out of the firewall due to exceeded authentication failures. This data is in the **Authentication - Locked Out Users** report.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) In the **Rule Objects** tree, expand the **Firewall Users** node.

4) Double-click **User Groups**. The **User Group** window is displayed.

5) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure external firewall groups

External groups are used in access control rules to restrict access to application or services through the firewall.

Create external groups that correspond to specific user groups on remote authentication servers in the **External Group** window. Then assign the external groups to the appropriate authenticator server by using the authenticator windows.

To use an external group in an access control rule, you must assign the group to an authenticator and then select that authenticator and the group when creating the rule.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) In the **Rule Objects** tree, expand the **Firewall Users** node.

4) Double-click **External Groups**. The **External Group** window is displayed.

5) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure MLC users

You can create a placeholder MLC user object because you do not currently see this object in the **Identity Browser**. Create this object in the **MLC User** window.

When you select an MLC user in the **Identity Browser** to use in an access control rule, the MLC user object is automatically created on the Control Center if it does not already exist. The object can then be used in other access control rules.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) In the **Rule Objects** tree, expand the **Firewall Users** node.

4) Double-click **MLC Users**. The **MLC User** window is displayed.

5) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure MLC groups

You can create a placeholder MLC group object because you do not currently see this object in the **Identity Browser**. Create this object in the **MLC Group** window.

When you select an MLC group in the **Identity Browser** to use in an access control rule, the MLC group object is automatically created on the Control Center if it does not already exist. The object can then be used in other access control rules.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) In the **Rule Objects** tree, expand the **Firewall Users** node.

4) Double-click **MLC Groups**. The **MLC Group** window is displayed.

5) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save this object.

Configure MLC distribution lists

You can create a placeholder MLC distribution list object because you do not currently see this object in the **Identity Browser**. Create this object in the **MLC Distribution List** window.

When you select an MLC distribution object in the **Identity Browser** to use in an access control rule, the MLC distribution list object is automatically created on the Control Center if it does not already exist. The object can then be used in other access control rules.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) In the **Rule Objects** tree, expand the **Firewall Users** node.

4) Double-click **MLC Distribution Lists**. The **MLC Distribution List** window is displayed.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

CHAPTER 14

Time periods

Contents

You can specify periods of time when an access control rule is in effect. Use the **Time Period** window to create these time periods.

Create time periods

You can create and maintain time periods. Time periods are used in access control rules to indicate when a rule is in effect.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Double-click the **Time Periods** node. The **Time Period** window is displayed.

   Tip: For option descriptions, press **F1**.

4) Enter a name and description for the **Time Period** object.
5) Select a type, and specify the days and times for the time period.
6) Click **OK**.

Result

The new **Time Period** object is added to the **Time Periods** node, and can be used in access control rules.

Related tasks

Access control rule management on page 301

CHAPTER 15

Virtual Private Network (VPN)

Contents

A Virtual Private Network (VPN) securely connects networks and nodes to form a single, protected network.

The data is protected as it tunnels through unsecured networks, such as the Internet or intranets. The VPN ensures data origin authentication, data integrity, data confidentiality, and anti-replay protection. A VPN works by encapsulating packets and sending them to a VPN peer for decapsulation. The encapsulated packets can be sent in the clear on the unsecured network between the VPN peers.

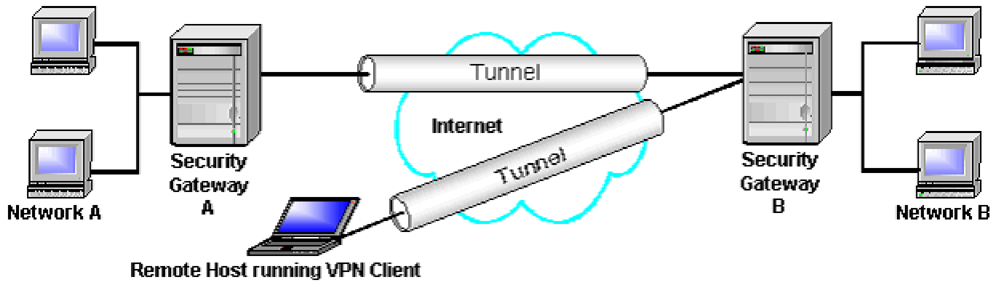
About VPN

The VPN is a security gateway between trusted and non-trusted networks that protects network access, network visibility, and network data.

The two types of supported VPN connections are *gateway-to-gateway* and *host-to-gateway*.

A gateway-to-gateway connection is often used when passing traffic from firewall to firewall between offices located in different cities. In this configuration, each gateway is identified by its IP address. Any end of the VPN can initiate and respond to a VPN connection. In the following illustration, the gateway-to-gateway tunnel connects networks A and B by way of Security Gateway A and Security Gateway B to form a VPN.

Figure 6: Gateway-to-gateway VPN example



In a host-to-gateway connection, one or more single remote hosts (also known as *road warriors*) connect to a protected network. This type of VPN access is often used to provide access to protected business-related services for external users, such as telecommuters, a company's mobile sales force, and extranet partners. VPN hosts are typically end-user (personal) computers equipped with IPsec-based VPN client software. The client software is invoked to establish a secure connection with the VPN. Unlike a gateway-to-gateway VPN which automatically allows either node to initiate or respond to a connection, a host-to-gateway VPN must be configured to allow secure connection initiated by the VPN client software. These connections are different from gateway-to-gateway connections because the physical IP address of the host is not always known in advance. In the above illustration, the host-to-gateway tunnel connects the remote host running a VPN client to Security Gateway B. If the remote host authenticates successfully, it can access resources in Network B. The administrator of Security Gateway B is responsible for setting up a security policy for the remote hosts.

VPN hosts initiate the negotiation with the Internet Key Exchange (IKE) service on the firewall. After the host is authenticated by IKE, the IPsec parameters are negotiated, and a secure tunnel to the firewall is established.

Client software for VPN hosts often has the capability of configuring a virtual IP address to use after communication with the security gateway is established. The virtual IP address is assigned to the VPN host user. This enables remote users to appear as internal users on a private network. When a virtual address is used, the source address of traffic originating from the VPN host is different from its physical address.

For more information on understanding the basics of VPNs, see the *VPN (virtual private networks)* section in the *Forcepoint Sidewinder Product Guide*.

VPN configuration sequence

When configuring a VPN, it is helpful to configure the component parts in sequence.

As a guide, define a VPN configuration in the following order:

1) Certificates.

2) Firewalls.

3) Client configuration objects.

4) VPN Wizard (peer objects and community objects).

More detailed descriptions of each step are found below.

VPN certificates

If your organization uses certificates to authenticate peers in its VPNs, configure those certificates before running the VPN Wizard or creating the necessary peers and community.

While you can occasionally request a certificate directly from an authentication window, the best practice is to have all certificates available before configuring the VPN components.

VPN firewalls

Each firewall window supports some global configuration information for all VPN configurations.

For each firewall, the firewall certificate management is handled in the Certificates area of the firewall-specific window. Server settings are also managed in this area. You can configure settings for the firewall Certificate server and assign certificates to various firewall-hosted servers that they then use to present when clients request a secure, authenticated connection.

Client configuration objects

A VPN client configuration is used to establish a network configuration for a VPN client so that it can operate on the private side of a firewall.

When a remote host connects to the firewall using a VPN client, you might want the host to appear as if it is located on an internal network (for example, a network behind the firewall). To provide this capability, you create one or more virtual subnets of IP addresses which can be assigned to remote clients as they successfully connect using a VPN. You can use host and subnet network objects to create the virtual subnet. You can also map fixed addresses to specified remote clients from the pool of virtual addresses. A fixed IP mapping enables a remote client to initiate a VPN, present identifying information, and then be assigned the fixed address. The fixed addresses that you specify must be within the range of available IP address as defined by the client configuration. Once an address is assigned, the remote client appears to be part of the protected network. The client configuration can also make specific DNS and/or WINS servers available to the client.

If you are creating a host-to-gateway VPN, create the necessary client configuration object before running the VPN Wizard or creating the necessary peers and community. You can then associate the communities with the appropriate firewall while you are using the VPN Wizard or creating the individual peers.

Using the VPN Wizard

The simplest way to create a VPN tunnel is to use the VPN Wizard.

This wizard takes you through creating the necessary peers, setting the required cryptographic parameters, and selecting the authentication method. When the wizard is completed, it adds a new community object and any new peer objects to the appropriate VPN areas. These objects can then be tweaked individually, without running the wizard again. (For firewalls, this process is the equivalent of creating a new VPN definition.)

Peer objects

Each VPN node and all or part of its protected domain is configured as a VPN peer by using the VPN Peer window. These defined VPN peers participate in VPN communities.

A *gateway* peer is that gateway that is described by its IP address, a set of protected networks behind it, and identities and certificates it presents during authentication. Gateway peers can consist of a managed firewall or an unmanaged gateway with a static IP address.

A *Road Warrior* peer (a set of VPN clients) is described by a set of protected networks, and the identities and certificates it presents during authentication. A Road Warrior peer may connect only to a gateway peer.

Community objects

VPN communities provide a mechanism for sharing VPN properties between two or more VPN peers. These properties include authentication methods, such as certificates and pre-shared keys; and cryptographic properties, such as IKE version and modes, encryption and hash strength, and other advanced options.

A *community* is a set of tunnels that share the same authentication and behavioral attributes. A community is described as a set of peers and a topology. The tunnel definitions are created automatically by combining pairs of peers according to the topology. These topologies correspond to the three types of VPN communities:

- **Mesh** — A *mesh* community is type of gateway-to-gateway VPN in which a secure tunnel is defined between all participating gateways. The mesh topology establishes a tunnel between each pair of peers.
- **Star** — A *star* community is a type of gateway-to-gateway VPN in which a secure tunnel is defined between the central gateway and each satellite gateway. The star topology uses a specified central peer and establishes a tunnel between it and each of the other peers. A star topology with only two peers is indistinguishable from a mesh topology. Secure tunnels are not defined between satellite gateways.
- **Remote access** — A *remote access* community is a host-to-gateway VPN. A secure tunnel is defined based on a specific interface of a particular firewall. The remote access topology requires exactly one gateway peer and one remote access peer. It is the only topology in which a remote host can participate. This model uses a peer object for the remote road warrior peer, but uses the community object to store information about the local gateway peer—which allows connections from the remote peer by opening an interface for the tunnel rather than knowing a remote peer address.

As a configuration convenience, a community can exist with less than two peers. This allows the operator to pre-configure specific future-use scenarios.

Related concepts

CA (certificate authority) certificate management on page 176

Access control rules for VPN traffic

In general, all packets that enter or leave the firewall by way of a VPN must pass through an access control rule.

On the firewall, if the packets that are coming into the firewall are to cross a zone boundary, you must create an access control rule to allow that traffic from its termination zone to its destination zone. A termination zone is where the traffic arrives from the VPN tunnel and is decapsulated. We recommend you use a virtual zone as the termination zone and then configure policy to move the unencrypted traffic from that zone to its appropriate destination. Because the default behavior of any firewall is to drop IP packets that do not match a configured access control rule, it is necessary to make sure that any tunneled traffic from remote gateways or hosts is covered by a corresponding access control rule. Configure access control rules by using the **Access Control Rule Editor** window.

Remote hosts, clients and Extended Authentication (XAUTH)

When a remote host is being used by an individual who is traveling or working from home, there is typically no way to know the IP address of the remote host's gateway or the IP address of the remote host itself. Special consideration may need to be given to VPN tunnels and rules for remote hosts.

Remote host configurations for VPN

VPN tunnel configurations for remote hosts specify a firewall interface as the peer. This allows phase 1 negotiations through the interface, regardless of the remote host's gateway IP address.

The corresponding VPN rule must specify the IP address of the remote host or the range of IP addresses in which the remote host can be found. To solve this problem, the VPN client software on the remote host must allow the user to specify a virtual IP address or must be able to accept an IP address that is dynamically assigned by the firewall.

To further enhance security, it is important that a user authenticates separately with the firewall. When possible, configure the VPN to use Extended Authentication (XAUTH). In addition to the normal authentication checks that are inherent during the negotiation process at the start of every VPN association, Extended Authentication goes one step further by requiring the person who is requesting the VPN connection to validate his or her identity. The Extended Authentication option is most useful if you have traveling employees who remotely connect to your network by using laptop computers. If a laptop computer is stolen, without Extended Authentication, it might be possible for an outsider to illegally access your network. This is because the information that is needed to establish the VPN connection (the self-signed certificate, and so on) is saved within the VPN client software. When Extended Authentication is used, however, a connection will not be established until the user specifies 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.

Client configurations for VPN

VPN client configuration objects are used to simplify the management of VPN clients. They do so by having the firewall manage certain configuration details on behalf of the client.

All that the client needs is the following information:

- Client software that supports ISAKMP mode-config exchange
- Authorization information (for example, a client certificate or a password)
- The address of the firewall

Here is how it works: you create a list of virtual subnets 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 that is available in the list. The firewall also negotiates with the client to determine other VPN requirements, such as the internal DNS and/or WINS servers that will be made available to the client. If the negotiation is successful, the client is connected and the VPN connection is established.

Not all VPN client software supports the negotiation of every client address pool parameter. Make sure that you verify that your client or clients support the necessary features.

You define the list of IP addresses available to the VPN client configuration. Even though the client might have a fixed IP address, the address that is used within the VPN tunnel is the address that has been assigned to it from the virtual subnet list. A client configuration can be used for fixed and dynamic clients.

Using Extended authentication (XAUTH) to validate identity

The Extended Authentication (XAUTH) option provides an additional level of security for remote access VPN clients.

In addition to the normal authentication checks that are inherent during the negotiation process at the start of every VPN association, Extended Authentication goes one step further by requiring the person who is requesting the VPN connection to validate his or her identity. The Extended Authentication option is most useful if you have traveling employees who connect remotely to your network by using laptop computers. If a laptop computer is stolen, without Extended Authentication, it might be possible for an outsider to illegally access your network. This is because the information that is needed to establish the VPN connection (the self-signed certificate, and so on) is saved within the VPN client software. When Extended Authentication is used, however, a connection will not be established until the user specifies 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.

On Control Center, XAUTH can be configured in two areas: in VPN communities that are configured for remote access and in VPN client configurations as a way of authenticating remote clients that are configured to use a fixed IP.

Create VPN tunnels

VPN Wizard creates mesh, star, and remote (road warrior) VPN tunnels. This wizard steps through the basic VPN configuration considerations without having to understand the more intricate details associated with configuring VPN tunnels using the VPN object model.

The resulting VPN tunnel configuration object can be viewed by inspecting the **VPN peers** objects, **VPN communities** objects, and **VPN client configurations** objects that are created as a result of using the wizard.

Note: Create all network objects and client configurations that are to be used in this VPN tunnel before you start the wizard. You might need objects to identify gateways, hosts, and endpoints. Because a firewall can be defined only once for each VPN tunnel configuration, identifying protected resources that are being made available might require pre-defining an endpoint group.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **VPN** node.

4) Double-click the **VPN Wizard** node. The **VPN Wizard** appears.

   Tip: For option descriptions, press **F1**.

5) Complete the fields for each page of the wizard. When you are finished with a page, click **Next**.

6) Review the summary, then click **Finish**.

Result

The wizard closes, and the VPN peer, community, client configuration, IKE and IPsec strategy objects that were configured in the **VPN Wizard** are created.

Manage firewall certificates for VPN gateways

You can manage the certificates for the selected firewall that will be presented by each VPN gateway.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **VPN** node.

4) Double-click the **VPN Wizard** node. The **VPN Wizard** is displayed.

5) Proceed through the wizard until you get to the **Authentication Configuration (Certificates)** page. In the list of certificates at the bottom of this page, click **Manage** for the VPN gateway to manage. The *firewall_name* Certificates window is displayed.

   Tip: For option descriptions, press **F1**.

6) Use the buttons on the right to add, remove and configure certificates.

7) Click **Close** to return to the **VPN Wizard**.

Related tasks
Create a security zone on page 64

Configure VPN peer objects

You can create peer objects that will participate in gateway-to-gateway and gateway-to-host VPN communities.

Note: You must create the needed network objects and client configurations before you configure a VPN peer object.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **VPN** node.

4) Double-click the **VPN Peers** node or right-click it and select **Add Object**. The **VPN Peer** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Enter a name or description for the **VPN peer** object, and select a peer type.

6) Specify address and authentication information for the peer.

7) Click **OK**.

Result

The new **VPN peer** object is added to the **VPN Peers** node, and can be used in VPN communities.

Add a VPN community

You can add a VPN communities object.

Note: Before adding a VPN community, make sure that the necessary VPN peers, hosts, and networks objects have been created.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **VPN** node in the tree.

4) Double-click **VPN Communities**. The **VPN Community** window appears.

   Tip: You can also right-click and select **Add Object** from the menu.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description, and select a community type.

6) Set the allowed authentication method for this VPN community. You can configure the community to use pre-shared keys or certificates, or both.

   a) Click the **Authentication** tab. The **Authentication** page is displayed.

   b) Select **Support Certificates** to use certificates as the authentication method for IKE phase 1 negotiations. When certificates are used as an authentication method, the certificates of the firewall and peer are exchanged, and the identity of each is verified. In addition to initial verification, constraints that must also be satisfied to begin IKE negotiations can be put on the peer's certificate.

   c) In the Trusted CA Certificates area, select the certificates from the certification authorities (CAs) that are trusted as issuers of the peer's certificate. This field displays all the CA certificates that have been imported into the firewalls. If the peer's certificate has been issued by a CA whose certificate is selected, the peer's certificate is accepted as authentic. If the issuer of the peer's certificate is not found among the selected CA certificates, the peer's certificate is rejected.

      Note: If this is version 7.x firewall and multiple CA certificates were defined on this firewall, when the firewall is retrieved, a dynamic CA certificate group is automatically created. This group is then automatically assigned to this firewall.

   d) Use the **Pre-Shared Key** field to specify the key that has been shared between the firewall and the peer. The key can be a maximum of 128 ASCII characters or 256 hexadecimal characters, excluding the 0x. It must be at least eight characters long and can consist of any valid characters. If hexadecimal representation is used, remember that an eight-bit value is represented by two hexadecimal characters. You are required to confirm this key after you analyze the configuration and click **OK**.

   e) Select **Use A-B Keys** to use A-B pre-shared keys as an authentication method for IKE phase 1 negotiations.

      If **Use A-B Keys** is selected, use the **Pre-Shared Key** field to specify the respective keys. The first portion of the A-B key (A Key) is specified into the **Pre-shared Key** field by the first administrator. The second portion of the A-B Key (B Key) is specified by having a second administrator log on and specify the second key in this field. Until the second key has been specified and the change has been applied to each managed firewall in the community, a warning message is displayed for the object to indicate that the A-B key pair is not complete.

7) Configure the key exchange properties that will be used for the VPN community.

   a) Select the IKE version and the mode used to establish an IKE phase 1 tunnel. In **Main** mode (the default), six packets must be exchanged to establish the phase 1 tunnel. In Aggressive mode, only three packet exchanges are required. **Aggressive** mode establishes the phase 1 tunnel faster, but **Main** mode provides greater protection against denial of service attacks.

   b) Determine whether you want to use the same or distinct cryptographic properties for phase 1 and phase 2 key exchange by selecting one of the following values:

      - To configure the same cryptographic properties for both phases, select **Configure Identical Phase 1 and Phase 2 Cryptographic Properties**.
      - To configure different cryptographic properties for each phase, select **Configure Phase 1 and Phase 2 Cryptographic Properties Individually**.

8) Use the **Cryptography** tab or tabs to configure the key exchange properties that will be used for the VPN community.

9) [Optional] Specify advanced options.

10) Click **Analyze** to validate your configuration. If you are satisfied with the analysis, click **OK** to save the VPN community object.

Result

Note: Some data validation is applied to make sure that all the required and conditionally required information has been specified. If you do not properly complete the VPN community configuration, an message is generated.

Create a network configuration for a VPN client

You can establish a network configuration for the VPN client to operate on the private side of a firewall.

When a remote host connects to the firewall using a VPN client, you might want the host to appear as though it is located on an internal network (for example, a network behind the firewall). To provide this capability, you create one or more virtual subnets 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 that are available in the virtual subnet. The firewall also negotiates with the client to determine other VPN requirements, such as the DNS and/or WINS servers that 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. Make sure to verify that your client or clients support the necessary features.

You define the number and size of the available virtual subnets. Even though the client might have a fixed IP address, the address that is used within the VPN definition is the address that has been assigned to it from the specified virtual subnet. The virtual subnet works for both fixed and dynamic clients.

You can also create multiple client configurations. You can group VPN clients into distinct virtual subnets to limit the resources that the clients in each group can access. In some cases, VPN client configuration objects can be used by more than one peer.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **VPN** node.

4) Double-click the **VPN Client Configurations** node or right-click it and select **Add Object**. The **VPN Client Configuration** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Use the **General** tab to configure a pool of virtual addresses to be used by remote peers when they attempt to make a VPN connection.

6) Use the **Fixed IP Mappings** to assign fixed addresses to selected clients.

7) Click **OK**.

Result

The new client configuration object is added to the **VPN Client Configurations** node.

Define fixed addresses for VPN clients

You can define fixed addresses for selected clients.

One of the benefits of assigning fixed IP addresses to selected clients is that you can govern what each client can do. For example, you might restrict access to certain clients, and you might grant additional privileges to other clients. Do this by creating a network object for a selected IP address and then using the network object within an access control rule.

Each unique IP address can appear in the fixed IP mappings table only once. Multiple identities representing a single client, however, can be mapped to one IP address.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **VPN** node.

4) Double-click the **VPN Client Configurations** node or right-click it and select **Add Object**. The **VPN Client Configuration** window is displayed.

5) Click the **Fixed IP Mappings** tab.

6) Click **Add** or **Edit**. The **VPN Client Fixed Mapping** window is displayed.

   Tip: For option descriptions, press **F1**.

7) Specify the address to be assigned to the client, and enter a description for the mapping object.

8) Specify the client identification strings for this entry.

   All entries listed in this area will be mapped to the associated IP address. Because a client can use one of several different IDs (a distinguished name, an email address, and so on) when negotiating a session, you can map multiple IDs to one IP address. However, you cannot map two separate clients to the same address.

   If you define all the possible IDs for a client, you will be ready, regardless of the ID that is presented during the negotiation. The following fields are available:

   Note: If a user will be using extended authentication, that user name will override any other ID.

9) Click **OK**.

Result

The new mapping is added to the **Fixed IP Mappings** table.

Add a VPN client configuration

You can add a VPN client configuration object. This object can be used when you create VPN Peer objects for a firewall and when you create VPN remote gateway objects.

When a remote host connects to the firewall using a VPN client, you may want the host to appear as if it is located on an internal network (for example, a network behind the firewall). To provide this capability, you create one or more *virtual subnets* 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 virtual subnet. 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.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **VPN** node.

4) Double-click **VPN Client Configurations**. The **VPN Client Configuration** window is displayed.

5) In the **Name** field, specify a unique name for the **VPN client configuration** object being created.

6) In the **Description** field, specify an appropriate user-defined description of the object being created.

7) On the **General** tab, specify the following information:

   a) In the **Virtual Subnets** list, select a previously defined interface, network, or address range that identifies the address range of possible addresses to be assigned to the clients that use this configuration.

   b) [Optional] In the **DNS Server** field, select the previously defined network object to serve as the DNS server for this configuration.

   c) [Optional] In the **NBNS/WINS Server** field, select the previously-defined network object to serve as the NetBIOS Name Server or WINS server for this configuration.

8) On the **Fixed IP Mappings** tab, click **Add** and select an IP address and the client identifier(s) to be used to identify a client connecting from the specified address. Repeat as necessary for this client configuration.

9) On the main **VPN Client Configuration** window, click **OK** to save the data.

Bypass IPsec policy evaluation

You can select certain traffic to bypass IPsec policy evaluation and to be sent outside of the encrypted tunnel. This traffic is defined based on its source and destination endpoints, which are represented as subnets. Other non-VPN access control rules will apply to this traffic.

Example: Traffic between two networks at two different sites is encrypted; however, you want traffic to and from the web server to be sent outside of the encrypted tunnel. You would configure a VPN bypass and place it in front of a more general definition in the VPN Definitions list.

Note: Unlike when you directly manage a firewall, you do not rank order the VPN definitions (tunnels) and bypasses. All VPN bypass objects are automatically processed before processing any VPN tunnels.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **VPN** node.

4) Double-click the **VPN Bypass** node. The **VPN Bypass** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description for the **VPN Bypass** object.

6) Select a firewall, zone, and local and remote networks.

7) Click **OK**.

Result

The new **VPN Bypass** object is added to the **VPN Bypass** node.

CHAPTER 16

Certificates

Contents

Use certificates 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 are used together with encryption to ensure that communication that is sent over a network is secure.

About certificates

Certificates are commonly used to associate a user or device with the appropriate public or private key pair for use with public key cryptography.

Public key cryptography, also known as asymmetric cryptography, is an encryption method where 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 the data that is encrypted by using the public key can be decrypted only by using the corresponding private key. Certificates and public key cryptography are used in the Secure Sockets Layer (SSL) protocol.

The Control Center uses certificates for:

- HTTPS content inspection
- HTTPS decryption
- VPN authentication and identity management
- Firewall administration services, such as the Forcepoint Sidewinder Admin Console, Endpoint Intelligence Agent, and the Control Center
- Miscellaneous services

The SSH proxy of the firewall also presents SSH host keys to SSH clients in the SSH Known Hosts window.

For firewalls, certificates are used by the following features:

- SSL Rules
- VPNs
- HTTPS Application Defense
- Forcepoint Sidewinder Admin Console
- Endpoint Intelligence Agent
- Cluster Registration Server
- Control Center Control
- Control Center Status

Certificate trust

The distinguished name (DN) of a certificate identifies the owner of the certificate. However, 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. To get a certificate signed:

1) The owner of the certificate submits the certificate to a CA.

2) The CA attempts to verify the following:
    - 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 identity and private key of the certificate holder, it signs the certificate.

Because the certificate has been signed by a CA, other parties know it can be trusted. For more information about distinguished names and their syntax, see the *Forcepoint Sidewinder Product Guide*.

Certificate file formats for importing and exporting

The Control Center supports the importation and exportation of certificates as binary or PEM-encoded X.509 files or as part of a PKCS-12 file. (A PKCS-12 file contains both a certificate and a private key and is normally protected with a password.)

The private key that is associated with a certificate can also be imported or exported, either as part of a PKCS-12 file or as a separate PKCS-1 or PKCS-8 file. The PKCS-10 format is also supported for requesting a certificate from a CA.

Firewall certificate server functions

The firewall certificate server performs several functions, including providing support for the certificate management daemon (CMD) and for an optional, external Lightweight Directory Access Protocol (LDAP) server.

If the LDAP function is configured, it can be used to automatically retrieve certificates and Certificate Revocation Lists (CRLs) from a Version 2 or Version 3 LDAP server. The firewall will attempt to retrieve any certificates and (optionally) any CRLs that it needs to validate certificates in a CA-based VPN. Note that the LDAP function is used only for non-Netscape Certificate Authorities (for example, Entrust). You can also control the level of audit that is generated by the certificate server.

The certificate server is managed in the **Certificates** area of the **Firewall** window.

Certificate management

There are several different types of certificates that can be managed on the Control Center Client application.

Each certificate has its own use:

- **Firewall certificate management** — Used to represent the identity of the firewall in SSL connections and VPN tunnels
- **Remote certificate management** — Used to identify peers who are involved with a VPN connection with a firewall and administrators who are using Common Access Card (CAC) authentication
- **CA (certificate authority) certificate management** — Used to authenticate the remote end of a VPN tunnel with private keys
- **Local CA certificate management** — Used by the Control Center Management Server in SSL rules to decrypt traffic

Firewall certificate management

Firewall certificates are used by the Control Center Management Server to represent the identity of the firewall in SSL connections and VPN tunnels.

You can manage these certificates on the **Firewall Certificates** tab on the **Certificates** area of the **Firewall** window.

Create a new firewall certificate

You create a new firewall certificate with a variety of signature mechanisms.

Steps

1) Navigate to the firewall that you are creating the certificate for.
   a) In the navigation bar, select **Policy**.
   b) Expand the **Firewalls** tree.
   c) Double-click the firewall that you want to create the certificate for. The **Firewall** window is displayed.
   d) In the navigation tree on the left, select **Certificates**. The **Firewall Certificates** tab is displayed by default.
2) Add the certificate.
   a) On the **Firewall Certificates** tab, click **Add Certificate**. The **Certificate Request Wizard** is displayed.

      Tip: For option descriptions, press **F1**.

   b) Follow the instructions in the wizard.
      In the **Signature Mechanism** field, select the mechanism and click **Next**.

      Note: If you selected **Manual PKCS10** as the signature mechanism, the text of the certificate request is displayed. You must copy and paste the displayed text into an online CA form or click **Save as** to save the certificate request to a file on your machine.

   c) Review your selections. To accept your selections, click **Next**. To make changes, click **Back**.

3) Click **Finish**. The certificate is created and is displayed on the **Firewall Certificates** tab in the **Certificates** area of the **Firewall** window.

4) The next step depends on your selection in the **Signature Mechanism** field:

   - If you selected **Manual PKCS10**, the status displayed is Pending: Awaiting Certificate Load. You must submit the certificate request to a CA. You must then load or retrieve the certificate by using the **Load Certificate Wizard** to complete this task.
   - If you selected **Self Signed**, the Control Center will sign and import the certificate. You have completed the creation of this certificate.
   - If you selected **CA Certificate**, the certificate is signed by the CA that you selected in the **CA Certificate** field on the **Signature Mechanism** page. For more information about CA certificates, see the procedure for importing a CA certificate.
   - If you selected **Control Center CA**, the certificate is signed by the default Control Center CA.

Related tasks

Load (retrieve) a firewall certificate on page 169

Import a CA certificate into the known certificates database on page 178

Import a firewall certificate

You can import an existing firewall certificate that is not currently in the Control Center Management Server database.

Steps

1) Navigate to the firewall that you are importing this certificate for.

   a) In the navigation bar, select **Policy**.

   b) Expand the **Firewalls** tree.

   c) Double-click the firewall that you want to import the certificate for. The **Firewall** window is displayed.

   d) In the navigation tree on the left, select **Certificates**. The **Firewall Certificates** tab is displayed by default.

2) Import the certificate.

   a) On the **Firewall Certificates** tab, click **Add Certificate**. The **Certificate Request** Wizard is displayed.

   Tip: For option descriptions, press **F1**.

   b) Follow the instructions in the wizard.

   In the **Import Mechanism** field, select the mechanism and click **Next**.

   - If you selected **File** as your import mechanism, you must specify the path and format of the certificate and private key. Then click **Next**.
   - If you selected **Encrypted File (PKCS12)** as your import mechanism, you must specify the path of the encrypted file, the password to access it, and whether to hide the password characters in the field (that is, they are displayed as asterisks). Then click **Next**.

c) Review your selections. To accept your selections, click **Next**. To make changes, click **Back**.

d) Click **Finish**. The certificate is created and is displayed on the **Firewall Certificates** tab in the **Certificates** area of the **Firewall** window.

3) Click **OK** in the **Firewall** window to save your changes.

Related tasks

Load (retrieve) a firewall certificate on page 169

Import a CA certificate into the known certificates database on page 178

Load (retrieve) a firewall certificate

Complete the certificate creation process by loading or retrieving a firewall certificate that was created by a certificate authority (CA) in response to a certificate enrollment request.

Note: Before you begin, the certificate enrollment request must be submitted to a CA. If the **Signature Mechanism** selection was Manual PKCS10, the certificate authority will send a certificate that you must then load.

Important: If Control Center manages the firewalls and the certificates are generated in Sidewinder, you must retrieve the certificates from Control Center. This exports the certificates to Control Center. If you fail to do so and apply policy, the firewall certificates are lost.

Steps

1) Navigate to the firewall that you are importing this certificate for.

   a) In the navigation bar, select **Policy**.

   b) Expand the **Firewalls** tree.

   c) Double-click the firewall that you want to import the certificate for. The **Firewall** window is displayed.

   d) In the navigation tree on the left, select **Certificates**. The **Firewall Certificates** tab is displayed by default.

2) Load or retrieve the certificate from a file or from an LDAP server.

   To load the certificate from a file:

   a) On the **Firewall Certificates** tab, select the certificate with the status of `Pending: Awaiting Certificate Load` and click **Load Certificate**. The **Load Certificate** wizard is displayed.

   b) Select **Load From File** and click **Next**.

   c) Specify the path of the certificate file or click **Browse** to navigate to the file. Then click **Next**.

   d) Review your selections. To accept your selections, click **Finish**. To make changes, click **Back**.

e) Click **Finish**. The certificate is loaded in the **Firewall Certificates** tab in the **Certificates** area of the **Firewall** window.

To load the certificate from an LDAP server:

a) On the **Firewall Certificates** tab, select the certificate with the status of **Pending: Awaiting Certificate Load** and click **Load Certificate**. The **Load Certificate** wizard is displayed.

b) Select **Load From LDAP Server** and click **Next**.

c) Specify the address, port, and distinguished name of the certificate on the LDAP server that you are loading or retrieving this certificate from and click **Next**. The Control Center Management Server issues a query command for your requested certificate.

d) Review your selections. To accept your selections, click **Finish**. To make changes, click **Back**.

e) Click **Finish**. The certificate is loaded in the **Firewall Certificates** tab in the **Certificates** area of the **Firewall** window.

View firewall and remote certificate details

You can view information about a firewall certificate or a remote certificate in the **Certificate Details** window.

Steps

1) In the navigation bar, select **Policy**.

2) Navigate to the type of certificate that you want to view.
To access the list of firewall certificates:

a) In the Policy tree, expand the **Firewalls** node.

b) Double-click the firewall that you want to view the certificate for. The **Firewall** window is displayed.

c) Expand the **Certificates** node. The **Certificates** area is displayed.

To access the list of remote certificates

a) In the navigation bar, select **Policy**.

b) Click the **Remote Certificates** tab. The **Remote Certificates** page is displayed.

3) Select a certificate in the table.

4) Click **Certificate Details**. The **Certificate Details** window is displayed.

Tip: For option descriptions, press **F1**.

5) Click **Cancel** to close this window.

Note: You can optionally change the name of this certificate. Some CAs do not support alternative names.

Export a firewall certificate

You can export the firewall certificate to 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.

You can export a firewall certificate several different ways when using the **Export Certificate** wizard:

- As a single file for the certificate only (with no private key)
- As a single file containing both the certificate and the private key
  This is the recommended procedure because this is the only procedure where both the certificate and the private key are encrypted.
- As two files — one for the certificate and one for the private key

> ⚠ **CAUTION:** The private key is not encrypted by using this procedure. It is important to protect the private key because 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) Navigate to the firewall that you are exporting this certificate to.
   a) In the navigation bar, select **Policy**.
   b) Expand the **Firewalls** tree.
   c) Double-click the firewall that you want to export the certificate to. The **Firewall** window is displayed.
   d) In the navigation tree on the left, select **Certificates**. The **Firewall Certificates** tab is displayed by default.
2) On the **Firewall Certificates** tab, select the certificate to be exported and click **Export Certificate**. The **Export Certificate** wizard is displayed.
3) Follow the instructions in the wizard.
4) Review your selections. To accept your selections, click **Next**. To make changes, click **Back**.
5) Click **Finish**. The certificate and its private key are exported separately as two files.

   > ⚠ **CAUTION:** The private key is not protected when it is individually exported. If you use a transportable medium to store the private key file, make sure that you destroy or reformat the medium after the private key information has been imported on the appropriate appliance.

6) Click **OK** in the **Firewall** window to save your changes.

Delete a firewall certificate

You can delete a firewall certificate on the **Firewall Certificates** tab.

> **Note:** The certificate is deleted *only* if it is not being used by a VPN, Application Defense, or other firewall component. If it is being used by one of these components, you will need to remove the certificate from the component or components before you can delete it.

Steps

1) Navigate to the firewall that you are deleting this certificate from.
    a) In the navigation bar, select **Policy**.
    b) Expand the **Firewalls** tree.
    c) Double-click the firewall to delete the certificate from. The **Firewall** window is displayed.
    d) In the navigation tree on the left, select **Certificates**. The **Firewall Certificates** tab is displayed by default.
2) On the **Firewall Certificates** tab, select the certificate to be deleted and click **Delete Certificate**. A confirmation message is displayed.
3) Click **Yes**.

Remote certificate management

Remote certificates identify two types of objects.

- VPN peers that are involved in a VPN connection with a firewall
- Administrators who are using authentication by a U.S. Department of Defense Common Access Card (CAC)

You can manage these certificates on the **Remote Certificates** page.

Related concepts
Certificate file formats for importing and exporting on page 166

Create a new remote certificate

You can create a new remote certificate with the **Certificate Request Wizard**.

Steps

1) Navigate to the **Remote Certificates** page.
    a) In the navigation bar, select **Policy**.

b) Click the **Remote Certificates** tab. The **Remote Certificates** page is displayed.

2) Add the certificate.

a) Click **Add Certificate**. The **Certificate Request Wizard** is displayed.

Tip: For option descriptions, press **F1**.

b) Select **Create a new certificate**, then click **Next**.

c) Follow the instructions in the wizard.
In the **Signature Mechanism** field, select the mechanism, then click **Next**.

Note: If you selected **Manual PKCS10** as the signature mechanism, the text of the certificate is displayed. You must copy and paste the displayed text into an online CA form or click **Save as** to save the certificate to a file on your machine.

d) Review your selections. To accept your selections, click **Next**. To make changes, click **Back**.

e) Click **Finish**. The certificate that you created is displayed in the table of certificates.

3) The next step depends on your selection in the **Signature Mechanism** field:

- If you selected **Manual PKCS10**, the status displayed is Pending: Awaiting Certificate Load. You must submit the certificate enrollment request to a CA. Only after you receive the certificate back from the CA can you then load or retrieve the certificate by using the **Load Certificate Wizard**.
- If you selected **Self Signed**, the Control Center will sign and import the certificate. You have finished with the creation of this certificate.
- If you selected **CA Certificate**, the certificate is signed by the CA certificate that is currently stored in the Control Center certificate database and that you had selected in this Wizard. For more information about CA certificates, see the procedure for importing a CA certificate.
- If you selected **Control Center CA**, the certificate is signed by the default Control Center CA. The default Control Center CA signs the SSL certificate that each firewall uses to communicate with the Control Center Management Server at port 9005.

Related tasks

Load (retrieve) a remote certificate on page 174
Import a CA certificate into the known certificates database on page 178

Import a remote certificate

You can import an existing remote certificate that is not currently in the Control Center Management Server database.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Remote Certificates** tab. The **Remote Certificates** page is displayed.

3) Click **Add Certificate**. The **Certificate Request** Wizard is displayed.

   Tip: For option descriptions, press **F1**.

4) Follow the instructions in the wizard.

   In the **Import Mechanism** field, select the mechanism and click **Next**.

5) The next page that is displayed depends on the value that you selected in the **Import Mechanism** field.
   - If you selected **File**, you must specify the path and format of the certificate, then click **Next**.
   - If you selected **Encrypted File (PKCS12)**, you must specify the path of the encrypted file, the password to access it, and whether to hide the password characters in the field (that is, they are displayed as asterisks). Then click **Next**.
   - If you selected **LDAP**, you must specify the address and port, of the LDAP Server where the certificate is saved. You must also specify the distinguished name that will be used to identify the certificate. Then click **Next**.

6) Click **Finish**. The certificate that you imported is displayed in the table.

Related tasks

Import a CA certificate into the known certificates database on page 178

Load (retrieve) a remote certificate

Complete the certificate creation process by loading or retrieving a remote certificate that was created in the Manual PKCS10 format.

Note: Before you can begin, the certificate enrollment request must be submitted to a certificate authority (CA). After you receive the certificate back from the CA, you can load or retrieve it.

Steps

1) Navigate to **Remote Certificates** page.

   a) In the navigation bar, select **Policy**.

   b) Click the **Remote Certificates** tab. The **Remote Certificates** page is displayed.

2) Load or retrieve the certificate from a file or from an LDAP server.

   To load the certificate from a file:

   a) Select the certificate with the status of `Pending: Awaiting Certificate Load` and click **Load Certificate**. The **Load Certificate** wizard is displayed.

   b) Follow the instructions in the wizard.

   c) Review your selections. To accept your selections, click **Next**. To make changes, click **Back**.

d) Click **Finish**. The certificate is loaded on the **Remote Certificates** page.

To load the certificate from an LDAP server:

a) On the **Remote Certificates** page, select the certificate with the status of **Pending: Awaiting Certificate Load** and click **Load Certificate**. The **Load Certificate** wizard is displayed.

b) Follow the instructions in the wizard.

The Control Center Management Server issues a query command for your requested certificate.

c) Review your selections. To accept your selections, click **Next**. To make changes, click **Back**.

d) Click **Finish**. The certificate is loaded in the table on the **Remote Certificates** page.

Export a remote certificate

Export a remote certificate when your users use a VPN client to establish a VPN connection between their machines and the firewall.

The VPN client requires the certificate to identify itself during the VPN connection negotiations. You can use the firewall to create a self-signed certificate for the VPN client. After it has been created, it can be converted to a new file format and then exported. At that point, it is imported to the VPN client program.

You can export a remote certificate several different ways when using the Export Certificate wizard:

- As a single file for the certificate only (with no private key)
- As a single file containing both the certificate and the private key. This is the recommended procedure because this is the only procedure where both the certificate and the private key are encrypted.
- As two files — one for the certificate and one for the private key

CAUTION: The private key is not encrypted by using this procedure. It is important to protect the private key because 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) Navigate to **Remote Certificates** page.

a) In the navigation bar, select **Policy**.

b) Click the **Remote Certificates** tab. The **Remote Certificates** page is displayed.

2) Select the certificate to be exported and click **Export Certificate**. The **Export Certificate** wizard is displayed.

Tip: For option descriptions, press **F1**.

3) Follow the instructions in the wizard.

4) Review your selections. To accept your selections, click **Next**. To make changes, click **Back**.

5) Click **Finish**. The certificate and its private key are exported separately as two files.

> **CAUTION:** The private key is not protected when it is individually exported. If you use a transportable medium to store the private key file, make sure that you destroy or reformat the medium after the private key information has been imported on the appropriate appliance.

Delete a remote certificate

You can delete a remote certificate on the **Remote Certificates** page.

Steps

1) Navigate to Remote Certificates page.
   a) In the navigation bar, select **Policy**.
   b) Click the **Remote Certificates** tab. The **Remote Certificates** page is displayed.
2) Select the certificate to be deleted and click **Delete Certificate**. A confirmation message is displayed.
3) Click **Yes**. The certificate is deleted *only* if it is not being used by a VPN, Application Defense, or other firewall component. If it is being used by one of these components, you must remove the certificate from the component or components before you can delete it.

CA (certificate authority) certificate management

On the firewall, certificates play an important role in allowing the use of automatic key generation in Internet Key Exchange (IKE) VPNs.

With 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 that you are negotiating session keys with is actually who it claims to be — a way to authenticate the other end of the VPN. To allow automatic key generation, the firewall can use pre-shared keys or certificates as the authentication method. Certificates are generally more reliable and tougher to spoof, and, therefore, are favored over shared passphrases (keys).

The firewall can use the following certificate trust sources:

- **Single certificate** — Single certificate authentication requires that the firewall generates a certificate and private key to be kept on the firewall and a certificate and private key to be exported and installed on a client. Each certificate, after it has been 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). Thus, it will trust any certificate that is signed by a particular CA that meets certain administrator-configured requirements for the identity contained within the certificate. Because of the nature of this type of policy, only locally administered Certificate Authorities should be used in this type of policy.

The default Control Center CA resides on the Control Center. Control Center uses it to sign the SSL certificate that is used by each firewall to communicate with Control Center on port 9005, requests made by the firewall to the Control Center to create certificates. When the firewall registers with the Control Center, it retrieves the Default_CC_CA object that represents the default Control Center CA certificate.

Certificate Revocation List (CRL)

The CRL is a list of subscribers who are paired with their digital certificate status.

The list enumerates revoked certificates along with the reason or reasons for revocation. The dates of certificate issue and the authorities that issued them are also included. In addition, each list contains a proposed date for the next release. When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user. Both certificates and CRLs are stored in repositories to make them accessible to users. LDAP servers, web servers, and FTP servers are examples of repositories.

You can configure the firewall certificate server to query a specified LDAP server for retrieving certificates and CRLs that are needed for certificate verification.

Use the **Certificates** area on the **Firewall** window to manage the CRL.

CA certificate management

For a firewall, when a VPN configuration is retrieved from the firewall, the content of the certificate, as well as the certificate name, is retrieved. This means that this CA certificate can be used in other firewall configurations without having to implicitly import the certificate into the firewalls.

When managing certificates by using the Control Center **Policy icon**, certificates are added and stored based on their function. These functional areas are:

- **Firewall certificates** — A firewall certificate is used to identify the firewall to a potential peer in a VPN connection, or to a client requesting a secure (SSL or HTTPS) connection. These certificates are created on a per-firewall basis by using the **Certificates** area in the **Firewall** window for each firewall. When creating a certificate for the firewall, you have the option to submit the certificate to a CA for signing, or have the firewall generate a self-signed certificate. The available actions in the firewall certificate area include requesting, loading, retrieving, viewing, exporting, and deleting certificates. You can also assign certificates to specific servers, such as the Forcepoint Sidewinder Admin Console server and the Cluster Registration server, and to the HTTP Application Defense.
- **Remote certificates** — A remote certificate identifies one or more peers that can be involved in a VPN connection with a firewall. These certificates are created by using the **Remote Certificates** page. The available actions in the remote certificate area include requesting, loading, retrieving, viewing, exporting, and deleting certificates. You are most likely to export a remote certificate if your users use a VPN client to establish a VPN connection between their machines and the firewall. The VPN client requires the use of a certificate to identify itself during the VPN connection negotiations. It is possible to use the firewall to create a self-signed certificate for the VPN client. After it is created, it can be converted to a new file format and then exported. From there, it is imported to the VPN client program.
- **CA certificates** — A certificate authority certificate is generally a root certificate that has been imported from a local or trusted CA server. These certificates are imported by using the CA Certificate Import Wizard. After the certificate has been imported, you can use the **Certificate Details** window to change a CA certificate's name and some of its information, such as its SCEP URL and CA ID. The identifier, such as its distinguished name, cannot be modified. CA certificates can also be exported for use as trust sources on clients.

Import a CA certificate into the known certificates database

Import certificates into the database of known certificates to use them for VPN authentication and as certificate authorities for certificates that are stored in the known certificates database.

Steps

1) Navigate to the **CA Certificate Import** Wizard.
   a) In the navigation bar, select **Policy**.
   b) In the lower left area of the window, click the **Rule Objects** tab.
   c) Expand the **VPN** node.
   d) Double-click the **CA Certificates** node. The **CA Certificate Import** Wizard is displayed.

      Tip: For option descriptions, press **F1**.

2) Follow the instructions in the wizard.
   - In the **Import Mechanism** field, select the mechanism and click **Next**.
     The next page that is displayed depends on the value that you selected in the **Import Mechanism** field.
   - If you selected **File**, you must specify the path of the certificate. Then click **Next**.
   - If you selected **SCEP**, you must specify the information about the SCEP server that you are sending the certificate to for signing. Then click **Next**.
   - If you selected **Netscape 4.2**, you must specify the URL of the Netscape certificate server. Then click **Next**.
   - Specify the type of retrieval method that is used to retrieve the certificate revocation lists (CRLs) from the selected CA. If you select a type, you must also specify the URL to use to retrieve the certificate revocation list (CRL) of the selected CA. Then click **Next**.

3) Review your selections. To accept your selections, click **Next**. To make changes, click **Back**.

4) Click **Finish**. The certificate that you imported is displayed in the list of CA certificates in the Rule Objects tree.

Edit a CA certificate

You can edit certain fields of an imported CA certificate. You can assign certificate names to actual certificate files and store this data in the database of the Control Center.

Note: After a CA certificate has been imported to the Control Center, the **Distinguished Name** field cannot be modified.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **VPN** node.

4) Expand the **CA Certificates** node. The list of certificate objects is displayed.

5) Double-click a **CA certificate** node. The **CA Certificate Details** window is displayed.

6) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

7) Click **OK** to save these changes.

Export a CA certificate

You can export the CA certificate to a remote peer. This allows the remote peer to recognize the firewall. On the remote peer, the certificate is imported as a root CA certificate.

Steps

1) Navigate to the **Export Certificates** wizard.

   a) In the navigation bar, select **Policy**.

   b) In the lower left area of the window, click the **Rule Objects** tab.

   c) Expand the **VPN** node.

   d) Expand the **CA Certificates** node. The list of CA certificate objects is displayed.

   e) Right-click the CA certificate to be exported and select **Export CA Certificate**. The **Export Certificate** wizard is displayed.

      Tip: For option descriptions, press **F1**.

2) Complete the wizard fields.

3) Review your selections. To accept your selections, click **Next**. To make changes, click **Back**.

4) Click **Finish**. The certificate is exported.

Delete a CA certificate

You can delete a CA certificate from the **CA Certificates** list in the **Rule Objects** tree.

Note: The certificate is deleted *only* if it is not being used by a VPN, SSL rule, Control Center MLC connection setting, Passport authenticator, or other firewall components. If it is being used by one of these components, you will need to remove the certificate from the component or components before you can delete it.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **VPN** node.
4) Expand the **CA Certificates** node. The list of CA certificate objects is displayed.
5) Right-click the CA certificate to be deleted and select **Remove Object(s)**. A confirmation message is displayed.
6) Click **Yes**.

Configure CA certificate groups

Manage and create CA certificate groups in the **CA Certificate Group** window. A CA certificate group contains multiple CA certificates. You can also define the firewalls that will have access to these groups.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **VPN** node.
4) Double-click the **CA Certificate Groups** node. The **CA Certificate Group** window is displayed.
5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this object.

Delete CA certificate groups

You can delete a CA certificate group from the **CA Certificate Groups** list in the **Rule Objects** tree.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **VPN** node.
4) Expand the **CA Certificate Groups** node. The list of CA certificate group objects is displayed.
5) Right-click the CA certificate group to be deleted and select **Remove Object(s)**. A confirmation message is displayed.
6) Click **Yes**. The certificate is deleted.

Local CA certificate management

Local CA certificates are used by the Control Center Management Server in SSL rules to decrypt and inspect SSL content.

A local CA certificate is different from a CA certificate because each local CA certificate on the Control Center Management Server contains a private key in addition to the CA certificate.

You can manage these certificates on the **Local CA Certificates** tab on the **Certificates** area of the **Firewall** window.

Create a new local CA certificate

You can create a new local CA certificate with the **Certificate Request Wizard**.

Steps

1) Navigate to the firewall that you are creating this certificate for.
    a) In the navigation bar, select **Policy**.
    b) Expand the **Firewalls** tree.
    c) Double-click the firewall that you want to create the certificate for. The **Firewall** window is displayed.
    d) In the navigation tree on the left, select **Certificates**. The **Firewall Certificates** tab is displayed by default.

2) Add the certificate.

   a) On the **Local CA Certificates** tab, click **Add Certificate**. The **Certificate Request Wizard** is displayed.

      Tip: For option descriptions, press **F1**.

   b) Follow the instructions in the wizard.

   c) Review your selections. To accept your selections, click **Next**. To make changes, click **Back**.

   d) Click **Finish**.

      The certificate that you created is displayed on the **Local CA Certificates** tab in the **Certificates** area of the **Firewall** window.

Export a local CA certificate

You can export the local CA certificate to a remote peer. This allows the remote peer to recognize the firewall. On the remote peer, the local CA certificate is imported as a remote certificate.

You can export a local CA certificate different ways when using the Export Certificate wizard:

- As a single file for the certificate only (with no private key)
- As a single file containing both the certificate and the private key. This is the recommended procedure because this is the only procedure where both the certificate and the private key are encrypted.
- As two files — one for the certificate and one for the private key

  CAUTION: The private key is not encrypted by using this procedure. It is important to protect the private key because 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) Navigate to the firewall that you are exporting this certificate to.

   a) In the navigation bar, select **Policy**.

   b) Expand the **Firewalls** tree.

   c) Double-click the firewall that you want to export the certificate to. The **Firewall** window is displayed.

   d) In the navigation tree on the left, select **Certificates** > **Local CA Certificates**. The **Local CA Certificates** tab is displayed.

2) On the **Local CA Certificates** tab, select the certificate to be exported and click **Export Certificate**. The **Export Certificate** wizard is displayed.

   Tip: For option descriptions, press **F1**.

3) Follow the instructions in the wizard.

4) Review your selections. To accept your selections, click **Next**. To make changes, click **Back**.

5) Click **Finish**.

> **CAUTION:** The private key is not protected when it is individually exported. If you use a transportable medium to store the private key file, make sure that you destroy or reformat the medium after the private key information has been imported on the appropriate appliance.

6) Click **OK** in the **Firewall** window to save your changes.

Delete a local CA certificate

You can delete a local CA certificate on the **Local CA Certificates** tab.

> **Note:** The certificate is deleted *only* if it is not being used in an SSL rule. You must remove the certificate from that component or those components before you can delete it.

Steps

1) Navigate to the firewall that you are deleting this certificate from.
   a) In the navigation bar, select **Policy**.
   b) Expand the **Firewalls** tree.
   c) Double-click the firewall that you want to delete the certificate from. The **Firewall** window is displayed.
   d) In the navigation tree on the left, select **Certificates** > **Local CA Certificates**. The **Local CA Certificates** tab is displayed.
2) On the **Local CA Certificates** tab, select the certificate to be deleted and click **Delete Certificate**. A confirmation message is displayed.
3) Click **Yes**.

CHAPTER 17

Responses to attacks and events

Contents

Use firewall attack responses and system event responses to monitor your network for abnormal and potentially threatening activities that range from an attempted attack to an audit overflow. You can configure the number of times that a particular event must occur within a specified time frame before it triggers a response.

About responses

When the firewall encounters audit activity that matches the specified type and frequency criteria, the response that you configure for that system event or attack type determines the way in which the firewall will react. An email and SNMP trap can alert the administrator, and packets from particular hosts can be blackholed, or ignored, for a specified period of time.

Some default attack and system event responses are automatically created on the firewall during its initial configuration. The additional configuration options you select will depend mainly on your site's security policy and, to some extent, on your own experiences using the features. You might want to start with the default options and make adjustments as necessary to meet your site's needs.

The following functions are available in the Control Center for different types of responses:

- **Responses** — Select this node in the tree on the **Rule Objects** tab to view the following subnodes:
  - **E-mail Accounts** — Select this node to view email accounts that will receive alerts during an attack response.
  - **Host Blackhole** — Select this node to view hosts from which suspect traffic will be blackholed, or ignored.
- **Attack Responses** — Select this option on the **Other Rules** tab of the **Policy** icon to view attack responses. These attack responses define the way that the firewall responds when it detects audit events that indicate such possible attacks as Type Enforcement violations and proxy floods. Configure and modify attack responses by using the **Attack Responses** page.
- **System Responses** — Select this option on the **Other Rules** tab of the **Policy** icon to view system responses. These system responses define the way that the firewall responds when it detects audit events that indicate such significant system events as license failures and log overflow issues. Configure and modify system responses in the **System Response** page.

Configure alert notification for email accounts

You can specify email accounts that will receive alerts during an attack response.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left corner of this window, click the **Rule Objects** tab.

3) Expand the **Responses** node.

4) Double-click the **E-mail Accounts** node. The **Responses - E-Mail Accounts** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description for the new email accounts object.

6) In the **Mail Recipients** field, enter on or more email accounts. Separate each account with a comma.

7) Click **OK**.

Result

The new email accounts object is added to the **E-mail Accounts** node, and can be selected when configuring attack or system responses.

Configure blackholes for suspected hosts

You can specify hosts from which suspect traffic is blackholed or ignored. The firewall blackholes traffic based on source address, rather than the type of traffic. If you blackhole a host, *all* traffic from that host will be ignored.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left corner of the window, click the **Rule Objects** tab.

3) Expand the **Responses** node.

4) Double-click the **Host Blackhole** node. The **Responses - Host Blackhole** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Enter a name and description for the new host blackhole object.

6) Select a time frame and a blackhole option.

7) Click **OK**.

Result

The new host blackhole object is added to the **E-mail Accounts** node, and can be selected when configuring attack or system responses.

View attack responses

You can view a complete list of the attack responses that have been defined on your system. To modify attack response settings, double-click the specific response.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab.

3) In the list, select **Attack Responses**. The **Attack Responses** page is displayed.

   Tip: For option descriptions, press **F1**.

Configure attack responses

You can configure and modify attack responses. Attack responses define the way that the firewall responds when it detects audit events that indicate such possible attacks as Type Enforcement violations and proxy floods.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab.

3) In the list, click **Attack Responses**. The **Attack Responses** page is displayed.

4) Double-click an attack response on the Attack Responses page. The **Attack Response** window appears.

   Tip: For option descriptions, press **F1**.

5) Make changes to the fields according to your policy.

6) Click **OK**.

Result

The changes to the Attack Response are saved.

Predefined audit filters for attacks

There are several predefined audit filters are used to detect attacks.

- **ACL Deny** — Detects when a connection is denied by a rule in the active policy.
- **Denied Authentication** — Detects when a user attempts to authenticate and specifies invalid data. For example, if a user is required to specify a password and specified it incorrectly, the denied auth event would log the event.
- **IPFilter Deny** — Detects when a connection is denied by the active filter policy.
- **IPS** — Detects severe attacks. This option also detects Application Defense violation attacks, buffer overflow attacks, general attacks, DOS attacks, policy violation attacks, protocol violation attacks, virus attacks and spam attacks. Severe attacks indicate something is occurring that an administrator should know.
- **Keyword Filter Failure** — Detects when an SMTP mail message is rejected due to a configured keyword filter.
- **Malicious Executable** — Detects a malicious executable sending traffic through the firewall.
- **Network Probe** — Detects network probe attacks, which occur any time a user attempts to connect or send a message to a TCP or UDP port that is not configured.
- **Proxy Flood** — 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 (network service sentry) 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.
- **Signature IPS Intrusion All** — Detects all attacks identified by the signature-based IPS. This category detects attacks that were denied, dropped, or rejected, as well as suspected attacks that were allowed, but were audited by IPS.
- **Signature IPS Intrusion Blackholed** — Detects attacks identified by the signature-based IPS, where the attacker was blackholed.
- **Signature IPS Intrusion Deny** — Detects attacks identified by the signature-based IPS, where the offending network session was dropped, or rejected, or the attacker was blackholed.
- **Spam Filter Failure** — Detects attacks of all severities that are spam.
- **TCP SYN Attack** — Detects a possible attempt to overrun the firewall with connection attempts.
- **GTI** — Detects attacks identified as spam by McAfee Global Threat Intelligence message reputation.
- **Type Enforcement** — Detects when there is a Type Enforcement violation due to an unauthorized user or process attempting to perform an illegal operation.
- **Unlisted Executable** — Detects unknown executable activity in the network and notifies the firewall.
- **Virus Filter Failure** — Detects attacks of all severities that are viruses.

View system responses

You can view a complete list of the system responses that have been defined on your system. To modify system response settings, double-click the specific response.

Steps

1) In the navigation bar, select **Policy**.
2) Click the **Other Rules** tab.
3) In the list, select **System Responses**. The **System Responses** page is displayed.

   Tip: For option descriptions, press **F1**.

Configure system responses

You can configure and modify system responses. System responses define the way that the firewall responds when it detects audit events that indicate such significant system events as license failures and log overflow issues.

Steps

1) In the navigation bar, select **Policy**.
2) Click the **Other Rules** tab.
3) In the list, click **System Responses**. The **System Responses** page is displayed.
4) Double-click an system response on the **System Responses** page. The **System Response** window appears.

   Tip: For option descriptions, press **F1**.

5) Make changes to the fields according to your policy.
6) Click **OK**.

Result

The changes to the System Response are saved.

Predefined audit filters for system events

There are several predefined audit filters used to detect system events.

- **HA failover** — Detects when a failover IP address changes because a High Availability (HA) 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 the hot processes (processes that consume too much CPU or memory) events.
- **IPsec Error** — Detects when traffic generates IPsec errors.
- **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.
- **Power Failure** — Detects when an Uninterruptible Power Supply (UPS) device detects a power failure and the firewall is running on UPS battery power.
- **UPS System Shutdown** — Detects when a UPS is running out of battery power or has been on battery power for the estimated battery time.

CHAPTER 18

Firewall settings

Contents

The **Firewall Settings** tab on the **Policy** icon contains a tree that displays all the objects that can be configured on a firewall.

You can create, edit, or delete these objects from this tree directly or you can edit the object from within the **Firewall** window. You can also drag an object from this tree to a specific firewall in the **Policy** tree.

Configurable firewall objects

Configurable firewall objects include settings for audit data, access control rule elements, scheduled tasks, and package updates.

The following objects can be configured.

- **Global Settings** — Specify a common group of features that can be applied to a number of Forcepoint Sidewinder firewalls. Features include a default Application Defense group, password and passport authenticators, zones, server and service settings, and virus scanning properties.
- **Audit Export** — Configure audit archive settings for a firewall by using the Audit Export window.
- **Firewall Syslog** — Configure the export of audit data to designated syslog servers.
- **Network Defenses** — Configure and maintain the audit data that the firewall generates for each of the specified protocols and the frequency with which to generate that audit.

- **Servers and Service settings** — Specify a network service that is associated with a server agent, or *daemon*, that is running on the firewall. Server services are created during the initial configuration of the firewall. They include services that are used for the following purposes:
  - Management of the firewall (for example, Admin Console)
  - Access to a networked service (for example, SNMP Agent)
  - Routing services (for example, gated, routed)
  - VPN connections (for example, ISAKMP server)
  - Firewall-specific functions (for example, cluster registration server), You can modify basic properties that are associated with these services. However, additional server services cannot be created.
- **IPS Signature Browser** — Specify the Intrusion Prevention System (IPS) signatures that have been installed. Use the IPS Signature Browser window to view and manage these signatures. You can also separately manage the signature settings and the signatures.
- **SmartFilter** — Specify SmartFilter settings and policies for a firewall.
- **GTI Reputation** — Specify global McAfee Global Threat Intelligence technology settings for access control rules.
- **Executable Reputation** — Define or retrieve an executable reputation object to apply across firewalls to compute reputation for an executable file.
- **Virus Scan** — Specify virus scanning properties. These properties include parameters for distributing scanner processes for incoming and outgoing traffic, controlling buffer sizes, handling archives, and scanning encrypted files.
- **Quality of Service** — Specify Quality of Service (QoS) profiles that contain one or more queues that you can use to prioritize network performance based on network traffic type.
- **DNS Zones** — Specify Domain Name System (DNS) zone objects that can be created and managed by a firewall.
- **Scheduled Jobs** — Specify jobs that can be scheduled to perform routine maintenance tasks on a firewall.
- **Third-Party Updates** — Specify a schedule on which the entities for the following content inspection methods are updated: virus scan updates, IPS signature updates, and Geo-Location updates.
- **Package Load** — Specify a schedule that can be used to check for the availability of packages on the download site. You can then download them to a firewall.

Configure common (global) settings

You can define a common group of features that can be applied to a number of firewalls. Such features include a default Application Defense group, password and Passport authenticators, zones, server and service settings, virus scanning properties, and other settings.

> **Note:** You can also define unique settings in the various tabs in the **Settings** page instead of using these global settings.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **Global Settings** node. The **Global Settings** window appears.

> **Tip:** For option descriptions, press **F1**.

4) Enter a name and description for the new global settings object.

5) Select values for firewall settings objects, rules objects, and other settings.

6) Click **OK**.

Result

The new global settings object appears beneath the **Global Settings** node. You can apply the new setting to a particular firewall on the **Settings** area of the **Firewall** window.

Configure audit archive settings for a firewall

You can define settings to automatically archive audit data from the firewall to the Control Center Management Server.

Audit archives are log files that contain a historical record of all suspicious and monitored network activity. Because these log files can grow very large over time, they need to be managed to prevent the hard disk from becoming full.

> **CAUTION:** Care is required when configuring frequent or numerous audit archives since this may result in possible system performance issues.

For the firewall, you can create an audit export configuration that specifies the information needed to export audit archives to a remote location (for example, location, protocol, format, target directory) and set up a schedule for exporting them. You can also configure settings that are needed to export the audit archives to the Control Center Management Server.

After you create an audit export configuration, you can select an audit export configuration for a particular firewall, export the audit archives for that firewall to the Management Server, and generate and view an audit report from the exported audit data.

Steps

1) Log on to the Control Center Client application.

2) In the navigation bar, select **Policy**.

3) In the lower left area of the window, click the **Firewall Settings** tab.

4) Double-click the **Audit Export** node. The **Audit Export** window is displayed.

> **Tip:** For option descriptions, press **F1**.

5) Configure audit export to the Control Center:

   a) In the **Name** field, type a name that identifies the export location, which is Control Center.

   b) On the **Export Locations** tab, select **Export to Control Center**.

   c) In the **Password** and **Confirm Password** fields, specify the password of the Control Center ftp account.

   d) [Optional] Click the **Frequency** tab to configure the frequency of the audit export. The default timeframe is hourly.

6) Click **OK**.

Result

The window closes, and the audit export configuration is saved.

Configure audit data export to syslog servers

You can configure the export of audit data to a designated syslog server.

Forcepoint Sidewinder uses the UNIX syslog facility to log messages that are sent by programs that are running on the firewall. These messages can be useful in tracking down unauthorized system users or in analyzing hardware or software problems. All syslog data is stored in the audit log files.

Listed below are some basic 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 also the types of messages that will be generated. Normally, applications generate messages of different severity levels, such as informational and critical.
- Malicious users will often try to edit syslog files to hide 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's audit log files.
- The log files that have been generated by syslogd can grow large in size and can start using large amounts of hard disk space. To solve this problem, the log files are periodically rotated.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **Firewall Syslog** node. The **Firewall Syslog** window appears.

   Tip: For option descriptions, press **F1**.

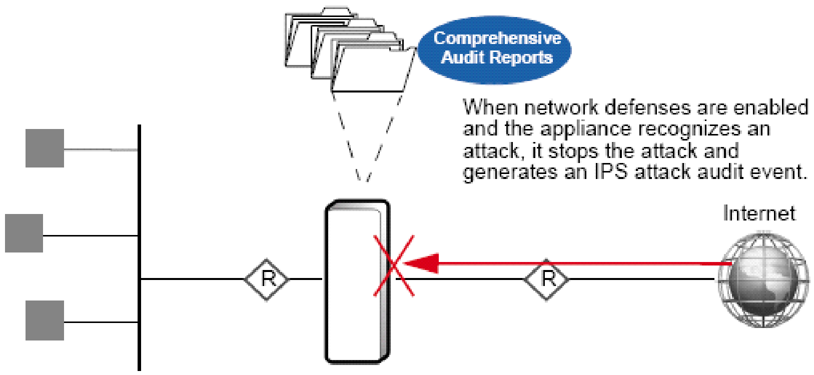
How network defenses settings work

Network defenses control the audit output for suspicious traffic at the data link, network, and transport layers that is detected by the firewall.

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.

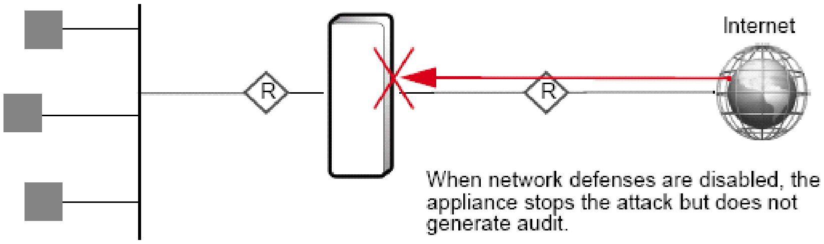
If network defenses are enabled, the audit reports provide detailed information on the denied traffic as shown below.

Figure 7: Enabled network defenses example


Comprehensive Audit Reports
When network defenses are enabled and the appliance recognizes an attack, it stops the attack and generates an IPS attack audit event.
Internet
R
R

If network defenses are not enabled, the firewall still stops suspicious traffic but does not generate audit, as shown in the following diagram.

Figure 8: Disabled network defenses example


Internet
R
R
When network defenses are disabled, the appliance stops the attack but does not generate audit.

After you decide to view the audit of these denied packets, you can configure the following options:

- Audit packets that the firewall determines to be part of an identifiable attack based on attack description (incorrect header length, incorrect redirect, and so on).
- 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.

Configure network defense audit reports

Configure and maintain the audit reports that the firewall generates for each of the specified protocols and the frequency at which to generate that audit.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **Network Defenses** node. The **Network Defenses** window appears.

   Tip: For option descriptions, press **F1**.

4) Configure options for specific protocols as necessary.

5) Click **OK**. The **Network** window closes, and saves any changes you made.

Result

The audit output reflects your changes.

Note: If no attacks are selected and no compliances issues are selected, the firewall still stops suspicious traffic but does not generate audit.

Server and service settings

Server services are created during the initial configuration of the firewall. They include services that are used for the following purposes.

- Management of the firewall (for example, Admin Console)
- Access to a networked service (for example, SNMP Agent)
- Routing services (for example, gated, routed)
- VPN connections (for example, ISAKMP server)
- Firewall-specific functions (for example, cluster registration server)

Managed firewalls and NTP

The Network Time Protocol (NTP) is an Internet standard protocol that enables client computers to maintain system time synchronization that is relative to master clocks.

Forcepoint Sidewinder appliances are compatible with NTP versions 2, 3, and 4. NTP version 4 is preferred and is used by default on the firewall.

The firewall can be configured as an NTP client or an NTP server. An NTP client receives time updates from another system; an NTP server supplies time updates to other systems. Typically, a firewall is configured as an

NTP client that receives time updates from an internal NTP server. Configuring a firewall to receive time updates from both an internal and an external NTP server is *not* recommended.

Configure servers and service settings

You can change the properties that are associated with server and service configurations.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **Server and Service Settings** node. The **Servers and Service Setting** window is displayed.

   Tip: For option descriptions, press **F1**.

4) Enter a name and description for the new servers and service settings object.

5) On each tab, configure the fields according to your policy.

6) When you have made all the necessary changes, click **OK**.

Result

The new server and service settings object is added to the **Server and Service Settings** node, and can be applied to managed firewalls.

IPS Signature Browser

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

You can perform the following actions:

- Globally enable or disable signatures
- View signature vulnerabilities on the Common Vulnerabilities and Exposures (CVE®) website

There are two objects beneath the **IPS Signature Browser** object in the **Settings** tree:

- **Default IPS Signature Browser** — This is the default signature object that is shipped with the Control Center.
- **Retrieved IPS Signature Browser**— This is the name of the object that is created when a retrieve from a firewall is performed. This object can contain user-defined signatures.

Globally enable or disable signatures

Create a signature browser object to determine the signatures that are disabled when this signature browser is associated with a specific firewall and is used in a policy.

By disabling a signature, you can possibly avoid false positives based on that signature (for example, when a certain signature is identifying legitimate traffic as an attack).

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **IPS Signature Browser** node. The **IPS Signature Browser** window is displayed.

   Tip: For option descriptions, press **F1**.

4) Enter a name and description for the new IPS Signature Browser object.

5) Deselect the checkboxes next to the signatures you want to disable.

   You can deselect multiple signatures by pressing and holding the **Ctrl key**.

   You can deselect a range of signatures by deselecting the first signature in the range, pressing and holding the **Shift key**, and then deselecting the last signature in the range.

6) Click **OK**.

Result

The new IPS Signature Browser object is added to the **IPS Signature Browser** node.

View signature vulnerabilities on the Common Vulnerabilities and Exposures (CVE®) website

You can view details about a vulnerability on the CVE list.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **IPS Signature Browser** node. The **IPS Signature Browser** window is displayed.

   Tip: For option descriptions, press **F1**.

4) Find the signature you want to view.

5) Look at the **Vulnerability** column for that signature. If CVE precedes the number, the vulnerability has been reviewed and accepted by CVE and is an official entry in the CVE list.

6) Click the link.

Result

The CVE webpage associated withe the signature opens in your web browser.

McAfee Global Threat Intelligence

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

McAfee 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, McAfee Global Threat Intelligence calculates a reputation value based on such attributes as sending behavior, blacklist and whitelist information, and spam trap information.

Reputation is expressed in the following classes:

- **Minimal Risk** (Low Risk) — Analysis indicates this is a legitimate source or destination of content or traffic.
- **Unverified** — Analysis indicates that this appears to be a legitimate source or destination of content or traffic, but also displays certain properties suggesting that further inspection is necessary.
- **Medium Risk** — Analysis indicates that this source or destination shows behavior that we believe is suspicious and content/traffic to or from it requires special scrutiny.
- **High Risk** — Analysis indicates that this source or destination does or will send or host potentially malicious content or traffic and we believe that it presents a serious risk.

Implement McAfee Global Threat Intelligence on your firewall to perform the following tasks:

- 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 access by authorized users who are inadvertently using external machines that are compromised.
- Evaluate external zones and internal zones with routable IP addresses.

Note: Private IP addresses are not evaluated by McAfee Global Threat Intelligence or examined in access control rules (for example, 10.x.x.x, 172.16.x.x, 192.168.x.x).

McAfee Global Threat Intelligence in allow access control rules

You can configure an *allow* access control rule to match these McAfee Global Threat Intelligence reputation classes.

- **Low Risk**

- **Low Risk** and **Unverified**
- **Low Risk**, **Unverified**, and **Medium Risk**

McAfee Global Threat Intelligence matches as indicated below:

- If the reputation score is within the selected reputation class or classes and all the 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 or classes, it is not a match. The connection is passed to the next access control rule.

McAfee Global Threat Intelligence in deny access control rules

You can configure a *deny* or *drop* access control rule to match these McAfee Global Threat Intelligence reputation classes.

- **High Risk**
- **High Risk** and **Medium Risk**
- **High Risk**, **Medium Risk**, and **Unverified**

McAfee Global Threat Intelligence matches as indicated below:

- If the reputation score is within the selected reputation class or classes 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 or classes, it is not a match. The connection is passed to the next access control rule.

McAfee Global Threat Intelligence access control rule example

You can use multiple McAfee 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 McAfee Global Threat Intelligence as shown in the table.

Table 12: Inbound SMTP access control rules using McAfee Global Threat Intelligence

Rule position	Rule action	Application reputation classes	Selected McAfee Global Threat Intelligence reputation classes
n	Deny or Drop	SMTP	High Risk
n+1	Allow	SMTP	Low Risk, Unverified, and Medium Risk

Auditing McAfee Global Threat Intelligence rules

An allow audit message is displayed in the audit log only if McAfee Global Threat Intelligence was used in the matching process for access control rules. It will *not* be added to the audit log for allowed connections under any of the following conditions:

- The source *and* destination IP addresses are on the McAfee Global Threat Intelligence whitelist.
- The connection is allowed by an access control rule that is earlier than a rule that uses McAfee Global Threat Intelligence.
- The connection does not match another element in the access control rule that uses McAfee Global Threat Intelligence (for example, the destination zone did not match). However, this same connection is allowed by a subsequent access control rule that does *not* use McAfee Global Threat Intelligence.

The following text is an example of the audit log text: `dest_reputation: 20`.

Configure McAfee Global Threat Intelligence settings for access control rules

You can create a **McAfee Global Threat Intelligence Reputation** object for use in access control rules.

McAfee Global Threat Intelligence Reputation objects contain settings for the reputation scores of IP addresses for inbound and outbound traffic.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **GTI** node. The **GTI Reputation** window appears.

   Tip: For option definitions, press **F1**.

4) Enter a name and description for the McAfee Global Threat Intelligence object.

5) In the **Whitelist** area, select object types, zones, or individual network objects to include in the McAfee Global Threat Intelligence whitelist.

   Selected objects will not be examined for McAfee Global Threat Intelligence reputation scores and will be exempt from the McAfee Global Threat Intelligence matching requirement of an access control rule.

   Note: Some objects are selected by default because your security policy probably defines allow and deny access control rules for these objects.

6) [Conditional] Select the **Audit traffic allowed by GTI** checkbox to include in the audit log those reputation scores of IP addresses for which connections are allowed.

   If the checkbox is selected and McAfee 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 is added to the audit log.

7) Click **OK**.

Result

The **McAfee Global Threat Intelligence Reputation** object is added to the **GTI Reputation** node and can be used in access control rules.

McAfee Endpoint Intelligence Agent

McAfee Endpoint Intelligence Agent (McAfee EIA) fetches data from an host endpoint and passes it to Sidewinder. Sidewinder validates and audits host information, uses it for policy decisions, and then enforces policies across the network.

Control Center helps you to configure Endpoint Intelligence Agent settings for a firewall. Control Center also provides a report of the connected hosts that are managed by a firewall.

Note: Endpoint Intelligence Agent is supported only on Sidewinder 8.3.0 or later.

Benefits

Endpoint Intelligence Agent collects user information associated with an application. Endpoint Intelligence Agent sends connection information, called *metadata*, that Sidewinder uses for policy decision making and auditing.

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 Endpoint Intelligence Agent 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 level for an executable file connection. Based on the score, firewall can configure attack responses and alerts for malicious or unknown executable files.

Deploying Endpoint Intelligence Agent

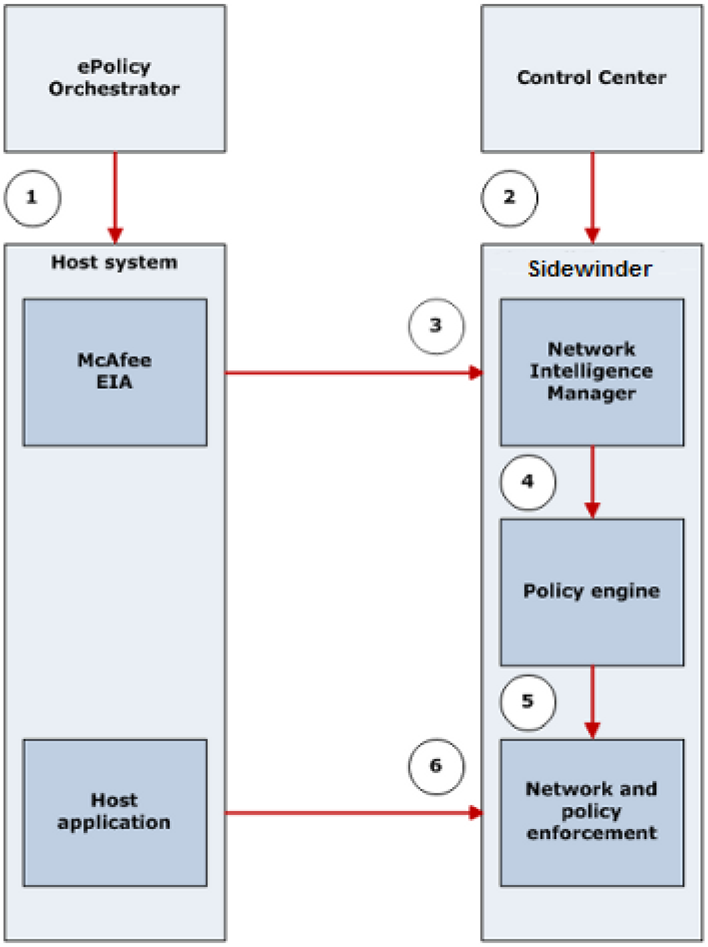
When Endpoint Intelligence Agent is installed on a host system, it monitors the system for any outgoing connections. When a connection attempt is made, the agent sends the metadata to Sidewinder over an encrypted channel.

Note: Endpoint Intelligence Agent currently provides metadata for TCP and UDP connections over IPv4.

Information like host application name, service name, and user information for each network connection are sent for processing to Sidewinder. The agent also provides attribute information like heuristic details (signedness, file size, and packedness), parent process, file description or application name for a signed file, and reputation score for an executable file and associated libraries.

McAfee ePolicy Orchestrator (McAfee ePO) manages Endpoint Intelligence Agent and deploys agents on multiple systems across the network.

Figure 9: Deploying Endpoint Intelligence Agent with Control Center



1) ePolicy Orchestrator installs and communicates with Endpoint Intelligence Agent on managed hosts.

2) The Control Center Management Server configures Endpoint Intelligence Agent for the firewalls.

3) The host agents send metadata to Sidewinder.

4) User information is used for authentication and policy enforcement. User information and other metadata is used for auditing.

5) Firewall processes and updates policies based on the metadata. Control Center applies these policies across the firewalls.

6) The host system initiates the network connection for the application. Sidewinder allows or denies the connection based on its policy.

Note: Endpoint Intelligence Agent is supported only on enterprise point product installations on the host systems. Consumer point product installations are not supported.

Communicating with Endpoint Intelligence Agent

Endpoint Intelligence Agent is used for auditing and identity control. Information like user identity and application details are extracted and used for auditing. The identity information is used at policy decision points. The attribute details are used to compute an executable file's reputation and enable Sidewinder to whitelist or blacklist an executable file and detect any new, unknown, and malicious applications in the network.

The Endpoint Intelligence Agent sends these details to the firewall:

- Source and destination address
- Protocol
- Source and destination port
- User information associated with the process
- Executable file name on the disk (full path)
- Executable file information (for only suspicious executable files)
  - MD5 hash value
  - File description
  - Signer
  - Signed time
  - File name (name from version table)
  - File version
- Malware analysis information
  - Malware risk level
  - Host heuristics
  - Host evidence data

For more details, refer to *McAfee Endpoint Intelligence Agent Product Guide*.

Understanding executable file reputation

When you run an executable file on the system, it generates network traffic. You want to determine whether an executable file can be trusted or not and only then allow it in the network.

If the executable file is safe, you want to allow it in the network and if it is unsafe, you want to take measures like blocking or raising alerts. You can use one or many reputation sources to determine trust in an executable file and set thresholds on the firewall. The level of confidence in an executable file derived based on these factors is termed as executable file reputation.

Related tasks

Enable executable file reputation on page 214

View reputation specific firewall audits on page 224

Using Endpoint Intelligence Agent to compute executable file reputation

Endpoint Intelligence Agent analyzes different characteristics of executable files and associated libraries (dlls) to determine an endpoint application's trust. You can also use reputation sources like GTI reputation and host reputation from Endpoint Intelligence Agent to compute an executable file's reputation.

You have to enable Endpoint Intelligence Agent to use this capability. Sidewinder can use executable file reputation to create a whitelist or blacklist database for auditing. This reputation also enables Sidewinder to generate alerts and reports for whitelisted, blacklisted, new, and unknown executables detected in the network.

Note: Executable file reputation is supported only on 8.3.2 EIA-enabled firewalls and later.

Benefits

Computing executable file reputation using Endpoint Intelligence Agent enables you to:

- Monitor executable files sending traffic from endpoints through firewall
- Detect new and unknown executable files in the network
- Determine confidence level for new and unknown executable files
- Create whitelists and blacklists for executable files on a firewall
- Evaluate overall confidence of an executable file based on reputation sources

Components of executable file reputation

You need to consider these factors to determine an executable file's level of confidence.

- Baseline computer profile from the Endpoint Baseline Generator to whitelist or blacklist executables
- Classification list that enables you to determine reputation for existing, new, and unknown executable files in the network
- Reputation sources like GTI reputation that provide reputation for executable files

Related concepts
Endpoint Baseline Generator on page 205
Classification list on page 207
McAfee Global Threat Intelligence on page 199

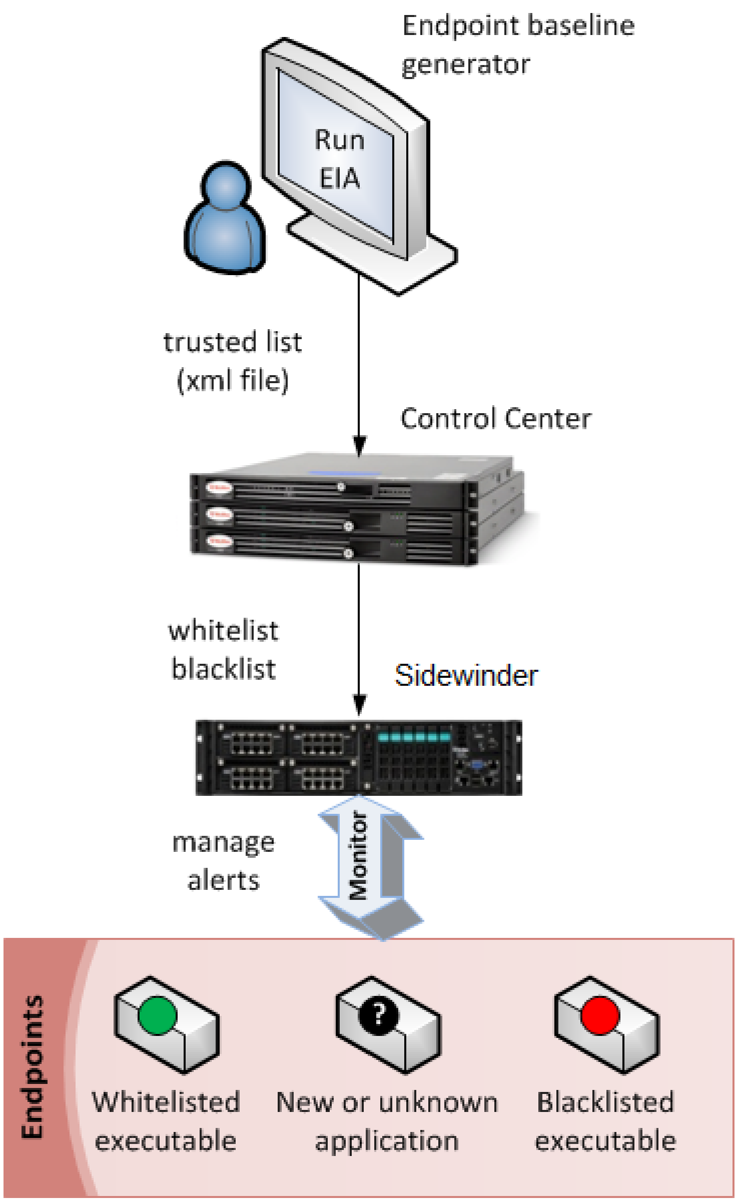
Endpoint Baseline Generator

The Endpoint Baseline Generator is an Endpoint Intelligence Agent tool that provides reputation scores to firewall. Endpoint Baseline Generator scans the system, calculates the heuristics for all the PE files, and generates an XML baseline computer profile (trusted list).

Note: Endpoint Baseline Generator supports scanning external hard drives with fixed media, for example, a hard disk drive or flash drive.

The .xml file has reputation scores that are used to set thresholds for whitelisting or blacklisting executable files and imported into the classification list. Based on this, Control Center or Sidewinder can define a whitelist or blacklist database on the firewall. This helps the firewall to monitor endpoint executable files and generate alerts based on their reputation.

Figure 10: Endpoint Baseline Generator workflow



For more details on Endpoint Baseline Generator, see the *McAfee Endpoint Intelligence Agent Product Guide*.

Baseline computer profile

The Endpoint Baseline Generator generates a baseline computer profile that classifies executable files based on confidence levels. This acts as a reputation source for Sidewinder to define a whitelist or blacklist database and monitor endpoint executable files.

The baseline computer profile .xml file provides information like MD5 hash value, endpoint file reputation, and heuristic bitmap. You can set thresholds and import the executable entries into the classification list .

Important: The .xml file is validated before importing it to the firewall.

The baseline computer profile has the executable files listed with their confidence levels and MD5 hash values in this format:

```
<MD5 value ='800b746fdc4d80469afc7e5e9b510c9c' name="msdia80.dll" version='8.0.50727.762'>
 <ProductName>New studio</ProductName>
 <ConfidenceLevel>2</ConfidenceLevel>
 <StaticBitmap>04aaaaabaa0200000000000000000000</StaticBitmap>
</MD5>
<MD5 value ='668b40abb178a7a2542567d8e0bccda4' name="Setup.exe"
 version='1.0.1'>
 <ProductName>Framework</ProductName>
 <ConfidenceLevel>6</ConfidenceLevel>
 <StaticBitmap>0ap3e46000a3e46000a3e46000a3e4600</StaticBitmap>
</MD5>
```

This table shows a mapping of confidence levels for executables files in the baseline computer profile to what confidence levels are displayed in the classification list .

Table 13: Confidence levels in the classification list

Confidence Level in classification list	Confidence levels in baseline computer profile
Very Low Risk	2
Unknown	0
Low Risk	3
Medium Risk	4
High Risk	5
Very High Risk	6

Classification list

The firewall settings allow you to define a classification list. A classification list is a list of whitelisted or blacklisted executable entries with their MD5 hash values.

You can import the baseline computer profile as-is or add executable entries to this list. You can also modify executable entries as whitelisted or blacklisted.

Confidence levels and thresholds

The classification list displays confidence level as a measure of risk of an executable file in the network. Valid values are:

- Very Low Risk— Risk level is very low
- Unknown
- Low Risk
- Medium Risk
- High Risk
- Very High Risk — Risk level is very high

Note: The confidence levels can't be modified and are imported as part of the baseline computer profile. By default, manual executable entries in the classification list set whitelist executable entries to **Very Low Risk** and blacklist executable entries to **Very High Risk**.

When you import executable entries, you can set the thresholds for whitelisting and blacklisting executable entries. Valid threshold values are:

- None
- Very Low Risk
- Unknown
- Low Risk
- Medium Risk
- High Risk
- Very High Risk
- All

You can set all executable entries to either whitelist or blacklist by setting the corresponding threshold value to **All**. Few things to remember while setting the threshold values are:

- If the whitelist or blacklist value is set to **All**, the blacklist or whitelist value must be set to **None**.
- Whitelist and blacklist values can never have the same threshold values.
- If the whitelist value is set to **Low Risk**, the blacklist value can be set to **Medium Risk** or **High Risk** or **Very High Risk**. Similarly, if the blacklist value is set to **Low Risk**, the whitelist value can be set to **Unknown Risk** or **Very Low Risk**.
- During import if you set the whitelist value to **Low Risk** and blacklist to **Medium Risk**, after import, the executable entries with values **Very Low Risk** and **Unknown** are whitelisted and those with values **High Risk** and **Very High Risk** are blacklisted in the classification list. This logic applies to all combinations of whitelist and blacklist threshold values.
- If the whitelist value is set to **Low Risk** and blacklist value is set to **High Risk**, the executable entries that do not fall in this whitelist-blacklist range are discarded.

Reputation sources

You can use sources like GTI reputation, Endpoint Intelligence Agent, and classification list to compute executable file reputation. These reputations are displayed on the **Dashboards** > **Summary** page.

You can use these reputation sources:

- **GTI Reputation** — When you select this checkbox, Sidewinder queries Global Threat Intelligence for an executable file's reputation. For more details, refer to the section on *McAfee Global Threat Intelligence* .
- **Executable Reputation** — When you select the **Classification List (below)** checkbox, whitelisted and blacklisted executable entries can used to compute reputation for an executable file. You can also import or manually add executable entries to the classification list.
- **Host Reputation** — Endpoint Intelligence Agent also acts as a reputation source and provides reputation scores for executable files. See the section on *Baseline computer profile* for more details.

These reputation sources are used to compute the overall confidence level and display the same in the **GTI** and **EIA** reports. Valid values for **GTI Reputation** are Very Low Risk, Unknown, Low Risk, Medium Risk, High Risk, and Very High Risk. Valid values for **Executable Reputation** are **Whitelisted** and **Blacklisted**.

Options for reputation objects

You can either modify a default executable reputation object, create a new object, or retrieve an existing executable reputation object from the firewall.

From the **Firewall Settings** tab, use one of these options:

- **Default Executable reputation** — You can use this object to create new or modify executable reputation objects. Double-click the object or right-click and select **Add Object** or **Edit Object** to create or modify an object.
- **Retrieved Executable Reputation** — You can retrieve an executable reputation object from a firewall. Select the firewall and right-click **Retrieve Firewall Objects** and select **Firewall Dialog Information**. The executable reputation object is retrieved and displayed under this node.

The executable reputation objects can be created and applied on firewalls using the **Policy** > **Firewalls** > **<firewall>** > **EIA** > **Executable Reputation** and **Policy** > **Firewall Settings** > **EIA Executable Reputation** > **<executable reputation object>** > **Apply on Firewalls** options.

Configure certificates for Endpoint Intelligence Agent

Certificate configuration is necessary for the encrypted communication between Control Center and Endpoint Intelligence Agent.

Use ePolicy Orchestrator as CA

Configure McAfee ePolicy Orchestrator as the Certificate Authority and configure Endpoint Intelligence Agent settings.

The certificate process consists of these high level steps:

1) Configure ePolicy Orchestrator as the Certificate Authority (CA).
   Follow the section, *Configure managed firewalls for ePolicy Orchestrator reporting* and ePolicy Orchestrator documentation.

2) Generate a certificate request.
   Refer to the section, *Create a new firewall certificate*.

3) Select **MaualPKCS10** as the signature mechanism.

4) Export the certificate as a *.p10 file for Endpoint Intelligence Agent.
   Refer to the section, *Export a firewall certificate*.

5) Sign the certificate in the ePolicy Orchestrator Extension for Sidewinder.

   Note: Endpoint Intelligence Agent 2.0.0 is compatible with ePolicy Orchestrator Extension for Sidewinder 5.3.2.

   Refer to ePolicy Orchestrator documentation.

6) Load the ePolicy Orchestrator signed certificate into Control Center.
   Refer to the section, *Load (retrieve) a firewall certificate*.

7) Apply the updated policy across the managed firewalls.

Note: If Control Center manages the firewalls and the certificates are generated in Sidewinder, you must retrieve the certificates from Control Center. This exports the certificates to Control Center.

Use Simple Certificate Enrollment Protocol (SCEP) as CA

From the ePolicy Orchestrator console, configure a SCEP server as the Certificate Authority and configure Endpoint Intelligence Agent settings.

The certificate process consists of these high level steps:

1) Configure a SCEP server as the CA.
   Follow the section, *Import a CA certificate into the known certificates database* and ePolicy Orchestrator documentation.

2) In Control Center, add the SCEP server as the CA.

3) Generate the certificate request and select **CA Certificate** as the signature mechanism. Select the SCEP CA to sign this certificate.
   Refer to the section, *Create a new firewall certificate*.

4) Control Center automatically sends the SCEP request, gets it signed, and imports the signed certificate.

5) Apply the updated policy across the managed firewalls.

Related tasks
Create a new firewall certificate on page 167
Import a CA certificate into the known certificates database on page 178
Export a firewall certificate on page 171
Load (retrieve) a firewall certificate on page 169

Configure Endpoint Intelligence Agent settings

Enable Endpoint Intelligence Agent for a firewall and configure settings to send metadata to Sidewinder.

Authentication options

Sidewinder works with Logon Collector to enforce policy based on the user information provided by Endpoint Intelligence Agent.

You can configure authentication settings for Endpoint Intelligence Agent 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 Endpoint Intelligence Agent authentication.

Configure authentication and certificate settings

Specify the certificates to be used for communicating with Endpoint Intelligence Agent and determine the authentication method to use.

Note: If you want to specify the zones and endpoints Endpoint Intelligence Agent responds to, create an explicit Endpoint Intelligence Agent communication rule before enabling Endpoint Intelligence Agent on the firewall.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Firewalls** node.

3) Double-click the firewall or right-click the firewall and select **Edit Firewall Settings**.

4) In the tree, click **EIA**. The **General Settings** tab options are displayed.

5) In the **Shared Key** field, type the shared key used in the communication between Sidewinder and Endpoint Intelligence Agent. This is pre-populated by default and needs to be the same between the host and firewall.

6) [Optional] Enable authentication.

   Tip: Set up passive mode in the Passport Authenticator to use this checkbox. Passive Passport must be enabled to use Endpoint Intelligence Agent 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 Endpoint Intelligence Agent is unable 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 to MLC**.

7) From the **Firewall Certificate** menu, select the firewall certificate that the host uses for verification.

8) From the **CA Certificate** menu, select the SCEP or ePolicy Orchestrator CA certificate.

9) [Optional] Select if the firewall needs to check for certificate revocation status and expired certifications while validating certificates.

10) Click **OK** to save your changes.

Discovery options

Endpoint Intelligence Agent hosts can dynamically discover the gateway firewall for a given route.

When a connection attempt is made, Endpoint Intelligence Agent 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 hosts selected under the **Discovery List** in the **Hosts and Discovery** tab to determine if the firewall will send a message to the Endpoint Intelligence Agent running on the host. This message tells the agent to send metadata to the firewall before sending the actual connection.

- If the **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 **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 **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 to discover firewall

Enable and configure discovery options on a firewall.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Firewalls** node.

3) Double-click the firewall or right-click the firewall and select **Edit Firewall Settings**.

4) In the tree, click **EIA**. The EIA settings are displayed.

5) Select **Enable Endpoint Intelligence Agent**.

6) Click the **Hosts and Discovery** tab.

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

7) Select **Enable Discovery**.

8) From the **Select network objects for discovery lists** list, select the network objects to configure for discovery.

9) From the **Discovery List**, select the network objects to whom you want the firewall to send the metadata request messages.

10) Under the **Active Hosts** list, view the connected hosts. Click **Refresh** to view the latest hosts.

11) Click **OK** to save your changes.

Configure executable file reputation

You can enable the firewall to accept and respond to the file reputation data received from Endpoint Intelligence Agent 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 Endpoint Intelligence Agent 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 blacklisted 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.

Using Global Threat Intelligence for executable files

When enabled, executable file connections from the host are compared to the Global Threat Intelligence reputation database. The firewall must be licensed for TrustedSource.

The firewall receives the MD5 hash value of each connection from Endpoint Intelligence Agent. The Global Threat Intelligence reports the reputation information about each file.

Using Classification list executable reputation matching

When enabled, executable file connections from the host are compared to the reputation classification list.

Note: The third source for reputation is the host reputation received from the Endpoint Intelligence Agent.

Enable executable file reputation

You need to create an executable reputation object and configure reputation sources to compute reputation for an executable file.

Before you begin

Go to **Policy** > **Firewalls node** > **<firewall>** > **EIA** and select the **Enable Endpoint Intelligence Agent** checkbox.

Steps

1) In the navigation bar, select **Policy**.

2) Expand the **Firewalls** node and double-click a firewall.

3) In the lower left area of the window, click the **Firewall Settings** tab.

4) Right-click on the **Executable Reputation** node and click **Add Object**. The Executable Reputation page is displayed.

5) Enter a name and description for the executable reputation object.

6) Select **Enable Executable Reputation**.

7) Select the reputation sources: **GTI Reputation** or **Classification List (below)** or both.

   Note: You can import executable entries or manually add executables to the classification list. The name attribute in the .xml must not have non-ASCII characters.

8) Click **OK**.

Result

The executable reputation object can be applied to firewalls using **Apply on...**.

Note: For load-balancing and load-sharing HA deployments, the reputation audits displayed on the **Dashboards** > **Summary** page are only from the member on which the DTLS connection is made.

Add an executable entry to the classification list

You can add individual executable entries to the classification list.

Before you begin

Go to **Policy** > **Firewalls node** > **<firewall>** > **EIA** and select the **Enable Endpoint Intelligence Agent** checkbox.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Expand the **Executable Reputation** node and double-click **Default Executable reputation**. The Executable Reputation page is displayed.

4) Enter a name and description for the executable reputation object.

5) Under **Classification List**, click **Add**. The Add Classification List page is displayed.

6) Enter a name for the executable file, select it as whitelist or blacklist, and enter the hash value. Click **Add**. You can click **Delete** to delete an entry or **Purge** to remove all the entries from the classification list.

   Note: The classification list is sorted by the filename.

   Note: By default, the whitlelist entries have the confidence level set as **Very Low** and blacklist entries have the confidence level set as **Very High** .

   Important: If two executable entries have the same hash value, at the time of addition, the latest entry overwrites the existing entry.

7) Click **OK**.

Result

The executable file is displayed in the classification list.

Import the baseline computer profile to the classification list

A classification list can have imported executable entries from the Endpoint Baseline Generator and manually added executable entries.

Before you begin

- Only a single Endpoint Baseline Generator database exists in an organization.
- The baseline computer profile is generated by the Endpoint Baseline Generator.
- The name attribute in the .xml must not have non-ASCII characters.
- Save the baseline computer profile on the system from where you plan to do the configuration.

Steps

1) From the Control Center Client application, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Expand the **Executable Reputation** node and double-click an object. The Executable Reputation page is displayed.

4) Under **Classification List**, click **Import**. The Import Classification List page is displayed.

5) Click **Browse** and navigate to the baseline computer profile .xml file.

   Note: We recommend that you import the baseline computer profile as-is and then modify the entries if needed.

   - Select **Add to existing list** if you want to append the executable entries to the existing classification list. By default, this checkbox is deselected. If this checkbox is deselected, the latest xml file overwrites the existing classification list.
   - Select **Ignore duplicate entries** to reject entries that have the duplicate hash values. By default, this checkbox is deselected. If this checkbox is deselected, the latest entry with the duplicate hash value overwrites the existing executable.

     Note: This checkbox is editable only when **Add to existing list** is selected.

6) Under **Classification Settings**, select the thresholds for whitelist and blacklist. Valid values are None, Very Low Risk, Unknown, Low Risk, Medium Risk, High Risk, Very High Risk, and All.

   Note: The whitelist and blacklist levels must be complementary. For example,

   - If the whitelist or blacklist value is set to **All**, the corresponding blacklist or whitelist value must be set to **None**.
   - If the whitelist value is set to **Low Risk**, the blacklist value can be set to **Medium Risk** or **High Risk** or **Very High Risk**. Similarly, if the blacklist value is set to **Low Risk**, the whitelist value can be set to **Unknown Risk** or **Very Low Risk**.

7) Click **Import**. The executable entries are imported into the classification list based on the import criteria.

   > **Note:** During import if you set the whitelist value to **Low Risk** and blacklist to **Medium Risk**, after import, the executables entries with values **Very Low Risk** and **Unknown** are whitelisted and those with values **High Risk** and **Very High Risk** are blacklisted in the classification list. This logic applies to all combinations of whitelist and blacklist threshold values.

8) Click **OK**.

Result

The imported executable entries are displayed in the classification list as whitelisted or blacklisted and their MD5 hash values.

Whitelist or blacklist an executable entry in the classification list

When you add or import executable files, you can whitelist or blacklist an executable entry. You can also modify an executable file as whitelisted or blacklisted.

Before you begin

An executable entry is added or imported into the classification list.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Expand the **Executable Reputation** node and double-click a reputation object. The Executable Reputation page is displayed.

4) From the **Classification List**, select an executable entry.

5) Click **Mark Whitelist** or **Mark Blacklist** based on your needs. A confirmation message pop-up is displayed. Click **Yes**.

   > **Tip:** Right-click on the grid and use **Select all** if you want to whitelist or blacklist all executable entries.

   > **Note:** Click **Delete** to remove an executable entry.

6) Click **OK**.

Result

The executable file's updated classification setting is displayed in the classification list.

Modify advanced firewall settings

Optionally, you can modify advanced settings for Endpoint Intelligence Agent, such as the maximum number of connected hosts, connection timeouts, and blackhole detection rate limits.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Firewalls** node.

3) Select and double-click a firewall or right-click a firewall and select **Edit Firewall Settings**.

4) In the tree, click **EIA**. The EIA settings are displayed.

5) Click the **Advanced Settings** tab.

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

6) Modify the settings as required.

7) Click **OK** to save your changes.

Next steps

You can now apply the changes to a firewall.

View active hosts

You can use Control Center to view the active hosts connected to Sidewinder.

Before you begin

Enable Endpoint Intelligence Agent.

View the active host IP addresses connected to the firewall.

Steps

1) In the navigation bar, select **Policy**.

2) From the **Firewalls** tree, select a firewall and right-click to select **Edit Firewall Settings**.

3) Select **EIA**. Click the **Hosts and Discovery** tab.

4) From the **Active Hosts as on <date and timestamp>** list, view the active hosts connected to the firewall.

Generate Active Hosts Report

You can use the host information to view the hosts connected to a firewall.

Steps

1) In the navigation bar, select **Monitor**.
2) In the **Reports** tab, go to **Firewall Reports**.
3) Select **Active Hosts**. The **Active Hosts** window is displayed.
4) From the **Firewall** drop-down menu, select a firewall.
5) Select the host parameters you want to view in the report.
6) Click **Request Report**.
    - Click **Save** to save the report
    - Click **Refresh** to view the latest report

Computing overall confidence for an executable file

The overall confidence level for an executable file is determined using reputations from various sources. It determines the extent to which an executable file is malicious or safe.

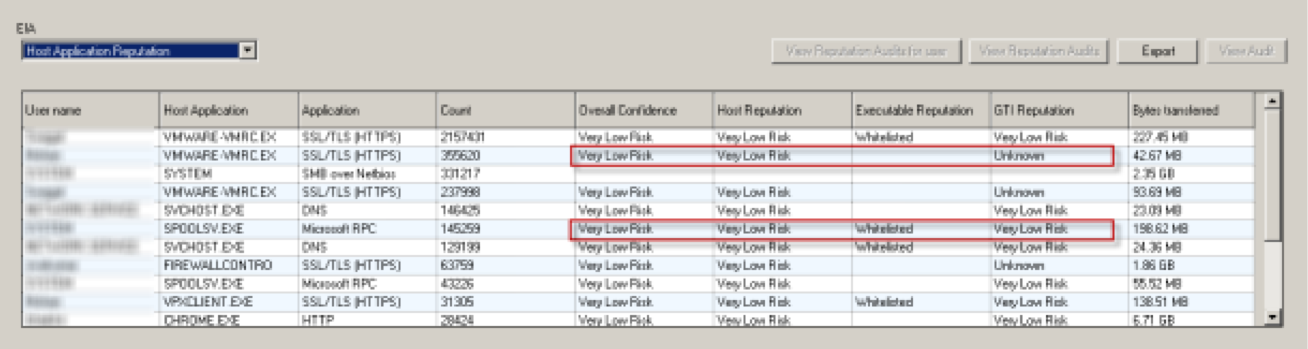
When a connection is made through the firewall, Endpoint Intelligence Agent supplies the heuristic data. The firewall checks the executable file MD5 hash value against the Global Threat Intelligence server and any entries on the classification list.

Overall malware confidence is calculated from these elements:

- **GTI Reputation** — Reputation of the executable file received from Global Threat Intelligence. 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.
- **Host Reputation** — Reputation of the executable received from Endpoint Intelligence Agent in the endpoint information. Endpoint Intelligence Agent on the host assigns the executable file MD5 a risk level rating: very low, low, medium, high, very high, or unknown.
- **Executable Reputation** — Reputation computed using the classification list (whitelisted and blacklisted). When the classification list is enabled, the executable is compared to the imported trusted list entries or manual entries.

On the **Dashboards** > **Summary** page, the overall confidence level for an executable file is displayed in the **GTI** and **EIA** reports. Host Reputation, Executable Reputation, and GTI Reputation details are also displayed in these reports.

Figure 11: Overall confidence level for executable files



EIA
Host Application Reputation

User name	Host Application	Application	Count	Overall Confidence	Host Reputation	Executable Reputation	GTI Reputation	Bytes transferred
[redacted]	VMWARE-VMRC.EX	SSL/TLS (HTTPS)	2157401	Very Low Risk	Very Low Risk	Whitelisted	Very Low Risk	227.45 MB
[redacted]	VMWARE-VMRC.EX	SSL/TLS (HTTPS)	355620	Very Low Risk	Very Low Risk		Unknown	42.67 MB
[redacted]	SYSTEM	SMB over Netbios	331217					2.35 GB
[redacted]	VMWARE-VMRC.EX	SSL/TLS (HTTPS)	237998	Very Low Risk	Very Low Risk		Unknown	93.69 MB
[redacted]	SVCHOST.EXE	DNS	146425	Very Low Risk	Very Low Risk		Very Low Risk	23.09 MB
[redacted]	SPOOLSV.EXE	Microsoft RPC	145259	Very Low Risk	Very Low Risk	Whitelisted	Very Low Risk	198.62 MB
[redacted]	SVCHOST.EXE	DNS	129199	Very Low Risk	Very Low Risk	Whitelisted	Very Low Risk	24.36 MB
[redacted]	FIREWALLCONTRO	SSL/TLS (HTTPS)	63759	Very Low Risk	Very Low Risk		Unknown	1.86 GB
[redacted]	SPOOLSV.EXE	Microsoft RPC	43226	Very Low Risk	Very Low Risk		Very Low Risk	55.52 MB
[redacted]	VPXCLIENT.EXE	SSL/TLS (HTTPS)	31305	Very Low Risk	Very Low Risk	Whitelisted	Very Low Risk	138.51 MB
[redacted]	CHROME.EXE	HTTP	28424	Very Low Risk	Very Low Risk		Very Low Risk	6.71 GB

Note: In the reports, **GTI Reputation** and **Executable Reputation** columns display valid values depending on the reputation sources selected on the executable reputation object page.

Existing endpoint executable files

Based on the trusted list, you have whitelisted and blacklisted the executables in your network. This table depicts a sample overall confidence matrix for executables based on signedness and GTI, host, and executable reputations.

Note: Other factors like signedness, heuristics, and evidence strings are also used to compute the overall reputation.

Overall Confidence	EIA Executable Reputation	Host Reputation	GTI Reputation	Signed / Trusted
Very High Risk	Any	Any	Very High Risk	
Very Low Risk	Any	Any	Very Low Risk	
Very Low Risk	Any	Any	Low Risk to High Risk range	Signed

New or unknown endpoint executable files

You have added some executable entries into the classification list. There are some new and unknown applications that are not in the GTI database and unrecognized by Endpoint Intelligence Agent. The table depicts a sample overall confidence matrix for such executables.

Overall Confidence	EIA Executable Reputation	Host Reputation	GTI Reputation	Signed / Trusted
Worst of all in the order of Very Low Risk, Unknown, Low Risk, Medium Risk, High Risk, and Very High Risk	Manual entries in the classification list Whitelist (Very Low Risk) Blacklist (Very High Risk)	Any	Low Risk to High Risk range	Not applicable
	Perform heuristics	Any	Unknown	Not applicable

Related tasks
View reputation specific firewall audits on page 224

Related information
Understanding executable file reputation on page 204

Firewall response

Once Sidewinder gets the overall confidence level for an executable file, it can take action. Sidewinder can create whitelist and blacklist databases for executable files, create malware rules, generate alerts, define attack responses, and view and analyze audits.

To configure how the firewall responds to the executable file connection reputation, you can configure an attack response.

From **Control Center** > **Alert Processing Rules** > **Firewall** list, use the **Malicious Executable Alert Rule** for filtering malware and **Unlisted Executable Alert Rule** to detect new executable files.

Table 14: Firewall actions

Whitelisted executables	Blacklisted executables	New or unknown executables
• Safe and allowed in the network • Add to whitelist and view audit	• Check the endpoint affected with the malware • Audit reputation and generate alerts • Add to blacklist and view audit	• Check the overall confidence level • Audit reputation and generate alerts based on severity • Add to blacklist or whitelist and view audit

For more details, see the *Forcepoint Sidewinder Product Guide*.

Interpreting reputation audits

In the firewall audit, you can view the specific evidence that contributed to the overall confidence score. The audit entries with an Endpoint Intelligence Agent 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 15: Host heuristic name and string format

Heuristic ID number	Heuristic name	Description	Heuristic string format
1	GTI	File reputation information received from Global Threat Intelligence server	Global Threat Intelligence has assigned this executable a <Medium | High | Very High> malware confidence.

Heuristic ID number	Heuristic name	Description	Heuristic string format
2	Signed File	File signed information	None
3	Minimum DLL imports found in executable	DLL imports found in executable file	An executable is typically linked to numerous libraries. This executable is linked to an unusually small number of libraries.
4	Resource section is missing	Resource Section information	An executable typically has a 'resource' section, which contains icons, menus, dialog boxes, etc. This executable does not have a resource section.
5	Embedded EXE/DLL found in the Resource section	Embedded executable file in resource section	An executable does not typically embed another executable. An embedded executable has been detected in the resource section of this executable.
6	Unknown resource in resource table	Unknown resource in resource section	An executable 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.
7	Executable packed or encrypted	Executable file packed or encrypted information	Malware is often encrypted or packed (compressed and encrypted) to avoid detection. This executable is encrypted or packed.
8	Executable writable section found	Executable file writable information	An executable is typically made up of read-only executable sections only. This executable has a writeable executable section.
9	Number of executable sections	Executable file section information	An executable is typically made up of one or two executable sections only. This executable has an unusually large number of executable sections.
10	Entry point is outside the default code section	Executable file entry point information	An executable typically starts its code execution from within its 'default executable' section. This executable is using an entry point outside its default executable section.
11	Section's size of raw data is zero	Size of raw data	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	File version name is different than actual file name	File version and actual name comparison	The file version name defined in the 'resource' section of this executable is different from the executable's actual filename.

Heuristic ID number	Heuristic name	Description	Heuristic string format
13	Suspicious File Locations	Suspicious file location	This executable is being run from a suspicious location on the file system, such as a temp folder.
14	Registry Run Entry	File autorun information	This executable is associated with autorun entries in the registry.
15	Anti-Debugging, Anti-Emulating, Anti-VM API	File using Anti-debugging API	This executable is using one or more API that is often used by malware to hamper analysis and avoid detection.
16	Executable-unknown	More than one unknown section name	A compiler typically generates standard section names (.code, .data, .bss, etc.) when it creates an executable. This executable has non-standard section names.
17	Executable suspicious	More than one suspicious section name	A compiler typically generates standard section names (.code, .data, .bss, etc.) when it creates an executable. This executable has non-standard section names that include special characters.
18	Overlay is packed	File overlay is packed	Data located after the last section of an executable is 'overlay' data, which is an easy target for malware writers. This executable has obfuscated overlay data.
19	Executable hidden	File is hidden	This executable has its 'hidden' file attribute set.
20	Executable extension	File has non-portable executable extension	This executable is in the Portable Executable (PE) format, yet it has a non-PE file extension (.jpg, .doc,.pdf, etc.).
21	Executable common name	File disk name is same as Windows common tool name	This executable has the same filename as a common Windows executable, but is running from a non-standard folder.

Each heuristic ID number is assigned a result in the **EIA Heuristic Report Viewer** window.

Table 16: Host heuristic results

Heuristic	Result
ID 1 GTI	• **Not Available** — Global Threat Intelligence is not found
ID 2 File signed	• **Not Available** — Signed file is not found • **Available, not used** — Signed file is not used

Heuristic	Result
ID 3-21 Heuristics	These IDs are used for heuristics. - **Ignored** — Heuristic ignored - **Skipped** — Not able to calculate Heuristic, possible error in the computation - **Not applicable** — Heuristic computation result negative - **Applicable** — Heuristic computation passed The IDs that are **Applicable** are displayed in the **Host_evidence** details. If none of the heuristics are applicable, the **Host_evidence** field is not displayed for an audit event.

View reputation specific firewall audits

From the **Dashboard** > **Summary** page, access firewall audit entries related to Endpoint Intelligence Agent.

Steps

1) In the navigation bar, select **Dashboards**. Click **Summary**.

2) View the list of recent audit entries for Endpoint Intelligence Agent.

   a) Scroll down to **EIA**.

   b) From the drop-down list, select either **Host Application Reputation** or **Malicious Host Application Reputation**.

   c) Select the time range.

   d) Click **Go**.

   > **Note:** If the name attribute in the imported .xml has non-ASCII characters, the reports might not display properly.

   e) Review the audit events using one of these methods:

   - **View Reputation Audits for user** — Select a user and click **View Reputation Audits for user**. This selection queries the audit for the host process name and the overall confidence score. Only the selected **user** is included in the results.
   - **View Reputation Audits** — Select an audit event and click **View Reputation Audits**. This selection queries the audit for the host process name and the overall confidence score. **All users** are included in the results.

     > **Tip:** The reputation audits are generated only for executables that have a correlation ID.

   - **View Audit** — Select an audit event and click **View Audit**. This selection displays the session audit.

   f) In the **Firewall Audit** window, select an audit event and click **Get Evidence**.

   g) Select an audit event and double-click to view the details in the **Firewall Audit Event Viewer** window.

   > **Note:** You can click **Back** to navigate to the Firewall Audit window.

h) Double-click **Host_heuristic** or **Host_evidence** to view more details in the **EIA Heuristic Report Viewer** window.

> **Note:** If none of the heuristics are **Applicable**, the **Host_evidence** field is not displayed for an audit event.

3) View the list of recent audit entries for executable files and their Global Threat Intelligence reputations.

a) Scroll down to **GTI**.

b) From the drop-down list, select either **Executable** or **Malicious Executable**.

c) Select the time range.

d) Click **Go**. Click **View Audit**.

e) In the **Firewall Audit** window, select an audit event and click **Get Evidence**.

f) Select an audit event and double-click to view the details in the **Firewall Audit Event Viewer** window.

g) Double-click **Host_heuristic** or **Host_evidence** to view more details in the **EIA Heuristic Report Viewer** window.

> **Note:** For load-balancing and load-sharing HA deployments, the reputation audits displayed on the **Dashboards** > **Summary** page are only from the member on which the DTLS connection is made.

Virus scanning

The virus protection service is used to configure access control rule-based MIME, virus, and spyware scanning. The virus protection service is a licensed, add-on module that uses a firewall-hosted virus scanner.

Use scanning services on HTTP traffic, HTTPS traffic, FTP files, and mail messages. When using scanning services, you can specify the number of server processes to be dedicated to various data sizes, allowing the firewall to process data more efficiently. You can also configure the interval of time at which to update the signature files.

Support for updating the virus protection engine and signature files is provided in the **Device Control** window. Support for scanning particular types of traffic (for example, HTTP, FTP, Sendmail) is provided in the **Application Defense** windows that are associated with those services:

- **FTP Application Defense** window — **Virus/Spyware** tab.
- **HTTP Application Defense** window — **MIME/Virus/Spyware** tab.
- **HTTPS Application Defense** window (not available for firewall versions 8.0.0 or later) — **MIME/Virus/Spyware** tab.
- **Mail (Sendmail) Application Defense** window — **MIME/Virus/Spyware** tab.

Configure global virus scanning properties

You can create a virus scan object for use in access control rules.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **Virus Scan** node. The **Virus Scan** window appears.

   Tip: For option definitions, press **F1**.

4) Enter a name and description for the virus scan object.

5) Configure the fields according to your policy needs.

6) Click **OK**.

Result

The new virus scan object is added to the **Virus Scan** node and can be used in access control rules.

Configure virus scanning signature updates

You can configure signature updates for a new third-party updates object for use in access control rules.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **Third-Party Updates** node in the tree. The **Third-Party Updates** window appears.

   Tip: For option definitions, press **F1**.

4) Enter a name and description for the new object.

5) Click the **A/V Signatures** row in the Updates List. The **A/V Signatures** tab is populated.

6) Complete the fields on the **A/V Signatures** field as needed for you policy.

7) Click **OK**.

Result

The new third-party updates object is added to the **Third-Party Updates** node, and can be used in access control rules.

Enable virus scanning on an access control rule

Configure virus scanning on an Application Defense and use the Application Defense in an access control rule.

Steps

1) Configure virus scanning on the appropriate Application Defense.
   a) In the navigation bar, select **Policy**.
   b) In the lower left area of the window, click the **Rule Objects** tab.
   c) Expand the **Application Defenses** node.
   d) Select the appropriate Application Defense type:
      - **HTTP** — Applies to HTTP-based applications and, for version 8.0.0 or later firewalls, HTTPS-based applications if decrypted by an SSL rule
      - **FTP** — Applies to FTP-based applications
      - **Mail (Sendmail)** — Applies to the Sendmail Server application
   e) Select an existing Application Defense or create a new one.
   f) Click the **MIME/Virus/Spyware** tab and configure it as appropriate.
   g) Save your changes.
2) Modify the appropriate access control rule.
   a) In the navigation bar, select **Policy**.
   b) Click the **Access Control Rules** tab.
   c) [Conditional] If you have a combination of version 7.x and 8.0.0 or later firewalls, click the tab of the access control rules with which you want to work.
   d) Double-click the access control rule for which you want to enable virus scanning or create a new access control rule.
   e) In the **Application Defense** field, select the Application Defense that you configured in Step 1.
   f) Save your changes.

Result

Virus scanning is now enabled on this access control rule.

Related tasks

Configure HTTP Application Defenses on page 89
Configure HTTPS Application Defenses on page 89
Configure FTP Application Defenses on page 86
Configure Mail (Sendmail) Application Defenses on page 91

Quality of Service

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.

Using the Quality of Service window, you can create QoS profiles that can be applied to the network interfaces of the firewall. Each QoS profile contains one or more queues that you can use to prioritize network performance based on network traffic type. Each queue is assigned a priority value, is allocated a percentage of available bandwidth, and can be allowed to borrow bandwidth from other queues. When a queue is full, any additional packets that match that queue are dropped. Queues are applied to network traffic based on the ports that are 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 want traffic for a particular port to be controlled in both directions, that port must be present in the QoS policy of both of the interfaces where traffic for that port leaves the firewall. The following QoS configurations are described to illustrate their effect on a connection between an internal client and external web server:

- The QoS profile for the external interface includes HTTP. Traffic that is sent from the internal client to the external web server is affected by QoS.
- The QoS profile for the internal interface includes HTTP. Traffic that is sent from the web server to the internal client is affected by QoS.
- Both the internal and the 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 port or ports that are configured in each queue. Protocols that use dynamic ports that are negotiated at the application layer (for example, FTP or VoIP) will not match QoS queues that use those ports because QoS does not examine the application layer when it processes packets.

Apply a QoS profile to a network interface

These high-level steps describe how to apply a QoS profile to a network interface.

Steps

1) Create a QoS profile (**Quality of Service** window).

2) Add QoS queues to the profile (**Quality of Service: Queues** window).

3) Apply the QoS profile to a network interface (**Firewall Interface** window from the **Firewall** window).

> **Note:** QoS cannot be configured on VLANs.

Create Quality of Service profiles

You can create a Quality of Service (QoS) profile that contains one or more queues that prioritize network performance based on network traffic type.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **Quality of Service** node. The **Quality of Service** window appears.

> **Tip:** For option definitions, press **F1**.

4) Enter an object name, profile name, and description for the new QoS object.

5) Configure the fields to fit the needs of your policy.

6) Click **OK**.

Result

The new QoS object is added to the **Quality of Service** node and can be selected on **Firewall Interface Properties** or **Cluster Interface Properties** pages.

Configure Quality of Service queues

You can create or edit a **Quality of Service** queue for use in **Quality of Service** objects.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **Quality of Service** node. The **Quality of Service** window appears.

> **Tip:** For option definitions, press **F1**.

4) Click (Add) or (Edit). The **Quality of Service: Queue** window is displayed.

5) Enter a name and description for the queue.

6) Configure the fields according to your policy.

7) Click **OK**.

Result

The window closes, and the new queue appears in the **Queues** list in the **Quality of Service** window.

DNS zones

A typical IPV4 address looks something like the following: 192.168.237.114.

This dotted decimal address is good for computing machines whose language is numbers. For humans, however, remembering numeric addresses for every computer to which they wish to connect is very cumbersome, if not impossible. What is needed is a system in which human-recognizable patterns can be used to represent IP addresses. This is where a Domain Name System comes in.

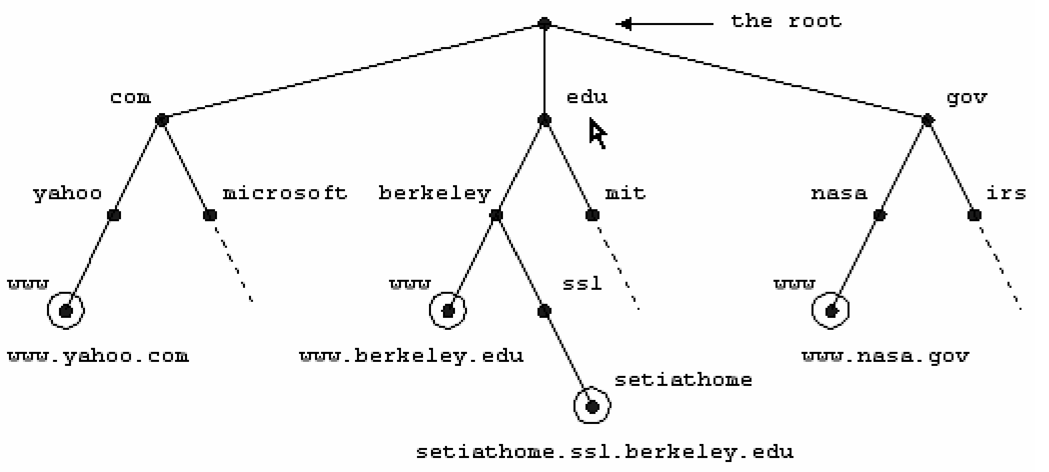
Domains, nodes, hosts, and the name space

For the purpose of administration, an IP network can be organized into logical partitions called domains. With the Internet, for example, there are separate domains for government information (.gov), educational information (.edu), and commercial information (.com) to name just a few.

The partitioning starts at what is called the root domain. All domains under the root domain (for example, as children of the root) are called top-level domains. Top-level domains can be partitioned into subdomains: second-level domains; second-level domains can also be partitioned into subdomains: third-level domains; and so on.

The Name part of Domain Name comes from the original need to create a mnemonic for IP addresses. Each domain and subdomain in the tree has a name assigned to it. Putting these concepts together results in something that looks like the following diagram:

Figure 12: Sample of the DNS name space of the Internet



In this figure, the following characteristics can be pointed out:

- com, edu, and gov are top-level domains. yahoo.com, microsoft.com, berkeley.edu, mit.edu, nasa.gov, and irs.gov are second-level domains. ssl.berkeley.edu is a third-level domain.
- A node is any dot in the preceding figure.
- A domain includes the node that defines the domain and all subdomains under that node. For instance, yahoo.com and microsoft.com are part of the com domain even though yahoo.com and microsoft.com are domains themselves.
- The nodes with circles are host names. www is a host name in the yahoo.com, berkeley.edu, and nasa.gov domains. setiathome is a host name in the ssl.berkeley.edu domain.
- A fully qualified domain name (FQDN) can be obtained by adding the host name to the domain name. This is seen with www.yahoo.com for instance. In fact, to truly be an FQDN, a name must also specify the root domain as a dot (.) on the end—for instance, www.yahoo.com.

Domain Name System (DNS)

After the logical structure and its rules were defined, a mechanism to manage the name-to-address mapping was created. For this purpose, a distributed database that is indexed by the domain names exists. This distributed database maps a host name to an IP address using all the components of the appropriate domain name.

The computers that contain portions of the database are called name servers. The name servers can contain the actual name-to-address mapping of some hosts. They can also contain pointers to other name servers that contain the name-to-address mapping of other hosts.

Domains versus zones

Each domain or subdomain can be divided into appropriate pieces to administrate that part of the name space.

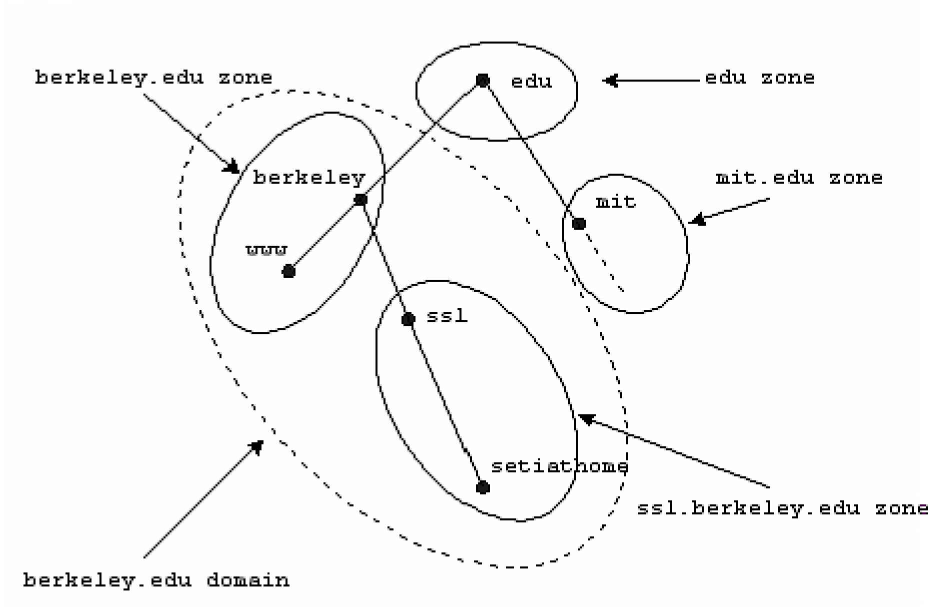
To illustrate this, look at the edu domain in the previous figure.

The organization that is responsible for the edu domain has broken it up into subdomains berkeley.edu and mit.edu. The administrators at Berkeley and MIT are now able to administer the name space for those universities as needed. Although this is true, the edu organization is still responsible for the part of the distributed database that maps the edu domain. Rather than loading the whole edu name space into the name servers of the edu organization, the edu organization can create zones. It might create an edu zone, a berkeley.edu zone, and an mit.edu zone. In this case, the edu zone does not contain any of the name-to-address mapping for Berkeley or MIT, only pointers to the name servers at Berkeley and MIT that contain the needed mapping.

Now, suppose that the administrators at Berkeley do not wish to hold the name-to-address mapping of the ssl.berkeley.edu domain on the main berkeley.edu name servers. They can, in turn, create another zone within their organization: the ssl.berkeley.edu zone. With this zone created, the main berkeley.edu name servers are free to contain only pointers to the ssl.berkeley.edu name servers for that part of the name space.

These ideas are shown in the following figure.

Figure 13: Possible zones of the sample *edu* domain



Notice that the ssl.berkeley.edu zone is in the berkeley.edu domain but is separate from the berkeley.edu zone.

The DNS name servers for a particular part of the name space can manage one or more zones.

Resource record types

Resource Record Types are used when configuring zone records that are associated with a particular zone by using the **DNS Zone window**.

The following table provides a list of resource record types that are most commonly used on the firewall.

The following resource record types defined in the table are not supported by the Forcepoint Sidewinder Admin Console:

- AAAA
- LOC
- RP
- SRV

Resource records follow the general format:

```
owner TTL class type data
```

or

```
owner class TTL type data
```

For the purpose of this example, `class` is always `IN` for Internet; `TTL`, or time-to-live, is optional; `owner` is also sometimes called `name`.

Table 17: Resource record types

Type	Owner (name)	Data	Purpose
*PTR pointer	The reverse zone name	The zone's domain name or the fully qualified domain name of a host.	This record is used for the address-to-name mapping that is needed to find a host name given an IP address.
*SOA Start of Authority	The zone's domain name	Master name server information	This record indicates to other name servers that this name server is authoritative for the zone.
A Address	The fully qualified domain name of a host	IP address	This record maps fully qualified domain names to IP addresses.
AAAA IPv6 Address	The fully qualified domain name of a host	IPv6 address	This record maps fully qualified domain names to IPv6 addresses.
CNAME Canonical Name	An alias fully qualified domain name	The real fully qualified domain name	This record creates an alias for a particular host.
HINFO Host Information	The fully qualified domain name of a host	A pair of strings identifying the host's hardware type and operating system	This record specifies the machine name and operating system name for a host.
LOC Location	The fully qualified domain name of a host	Latitude, longitude, and altitude	This record specifies the physical location of a host on the planet.
MX Mail Exchanger	The zone's domain name	A preference number and the fully qualified domain name of the mail server	This record specifies the mail exchange servers that are available for a zone.
NS Name Server	The zone's domain name	The fully qualified domain name of the name server	This record specifies an authoritative name server for the zone.
RP Responsible Person	The zone's domain name or the fully qualified domain name of a host	The email address (in domain name format) and the fully qualified domain name of a host with additional information (in TXT records)	This record indicates who is responsible for a host or zone.
SRV Service	The service and protocol name followed by the host name	Priority, weight, port number, and fully qualified domain name for the host that carries the service	This record maps a service like FTP or HTTP to one or more hosts. The hosts can be given priority and weight to facilitate load distribution.
TXT Text	The fully qualified domain name of a host	Text strings	This record is used to present textual information about a host.

***SOA** records are generated automatically by the firewall. **PTR** records are generated if you select the **Generate PTR Records** checkbox on the Configuration tab of the **DNS Zone window**, or they are allowed if you select the **Reverse Zone** checkbox on that page.

Resource record example

The following example should be used as a guide when creating or defining resource records.

CAUTION: A resource record without a value in its **Name** field takes the name of the preceding record. The NS (Name Server) record that is created automatically by the firewall is at the top of the list but has no name; consequently, it takes the name of the **SOA** (Start of Authority) record that is also created automatically by the firewall but not shown on the **Resource Records** tab of the **DNS Zone** window. The name of the **SOA** record is obtained from the **Domain Name** and **Name server advertisement** parameters that are set on the **Configuration** tab of the **DNS Zone** window.

The following table shows an example of resource records.

Table 18: Resource records example

Order	Name	Type	Data	TTL	Enabled
1		NS	nameserver		X
2		MX	10 mailserver1		X
3	nameserver	A	10.1.0.2		X
4	mailserver1	A	10.1.0.3		X
5	www	A	10.1.0.3		X
6	mail	CNAME	mailserver1		X
7	ftp	CNAME	www		X

Notice that the NS record in Entry 1 does not have a name; therefore, it takes the name of the SOA record that is created by the firewall. The MX record in Entry 2 takes the name of the NS record in Entry 1.

If you change the order of the resource records in the table, you must make sure that unnamed records are placed in a position that gives them the desired name.

Configure DNS zones

You can create a DNS zone object for use in configuring managed firewalls.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **DNS Zones** node. The **DNS Zone** window appears.

Tip: For option definitions, press **F1**.

4) Enter an object name, domain name and description.

5) Specify zone properties as needed for your policy.

6) Click **OK**.

Result

The new **DNS zone** object is added to the **DNS Zones** node, and can be used when configuring DNS for managed firewalls.

Schedule jobs

Schedule jobs that perform routine maintenance tasks on a firewall.

The tasks you can schedule include exporting audit log files, installing or rolling back software updates, downloading available patches, checking status of licenses, and updating Virus Scan and IPS (Intrusion Prevention System) signature files. Scheduled jobs are run by the `cron` daemon.

You may select the frequency with which jobs are run (for example, hourly, daily, weekly), or you may create a custom schedule for running them (for example, check system audit partition use at five minutes past every hour of every day).

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **Scheduled Jobs** node. The **Scheduled Jobs** window is displayed.

   Tip: For option descriptions, press **F1**.

4) Enter a name and description for the new Scheduled Jobs object.

5) On the **Firewall Crontab** tab, select the jobs to be scheduled and the frequency at which they will be run.

   Note: Each job must be able to be set so that the job can run at multiple, discrete times throughout the year. One-time tasks cannot be scheduled.

6) On the **Scheduled Backup** tab, schedule automatic configuration backups.

   You can back up configuration files to the firewall, a USB drive, a remote system, or a remote Control Center Management Server.

7) Click **OK**.

Result

The Scheduled Job object is added to the **Scheduled Jobs** node and can be applied to firewalls.

Configure third-party update schedules

Configure a schedule for updating virus protection signature files, application signatures files, IPS (Intrusion Prevention System) signature files, Geo-Location network objects, messages from Forcepoint, and SmartFilter categories and SmartFilter database updates from the download server.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **Third-Party Updates** node in the tree. The **Third-Party Updates** window is displayed.

   Tip: For option descriptions, press **F1**.

4) Enter a name and description for the new **Third-Party Updates** object.

5) For each update you want to modify:

   a) Select the update in the **Updates List**.

   b) Make any changes at the bottom of the window.

6) When you are finished making your changes, click **OK**.

Result

The new **Third-Party Updates** object is added to the **Third-Party Updates** node, and can be applied to managed firewalls.

Establish a schedule to check for software updates

Establish a schedule to check for the availability of packages on the download site and to download them to a firewall.

You can then use the **Control Center** icon to schedule downloaded packages for installation on the firewall.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Double-click the **Package Load** node in the tree. The **Package Load** window is displayed.

> **Tip:** For option descriptions, click **F1**.

4) Enter a name and description for the new **Package Load** object.

5) Configure the fields in accordance with your policy.

6) Click **OK**.

Result

The new **Package Load** object is added to the **Package Load** node and can be applied to managed firewalls.

CHAPTER 19

Firewalls

Contents

Firewall objects represent the physical devices that are used to implement a security policy for an organization. They are designed to protect organization IT infrastructure by keeping out unauthorized users, code, and applications, both internally and externally.

About firewalls

In the Control Center, firewall objects represent the configuration data and characteristics that are specific to a single firewall.

Creating firewall objects is a two-part process:

1) All types of firewall objects that represent physical devices in your configuration must be identified by providing basic information. Use the **Add New Firewall** window or the **Sign Up Firewalls** window to accomplish this task.

2) All the object-specific configuration information must be created for or retrieved from each firewall. Use the **Firewall** window to manage firewall configuration information.

Use the Control Center to obtain the configuration information directly from previously configured firewalls. You can select the specific configuration components to retrieve from a particular firewall. The information that has been retrieved is converted into Control Center objects and is then displayed in the associated areas of the **Firewall** window.

The Control Center has two ways to read configuration information directly from the firewall, to normalize the data, and to store this information in the database. You can retrieve configuration information when adding the firewall or at a later time.

Use the firewall to connect your organization to the Internet while protecting your network from unauthorized users and attackers, while also protecting internal users as they access the Internet. The firewall combines an application-layer firewall, IPsec VPN capabilities, web filtering (SmartFilter software), global-reputation-based filtering (McAfee Global Threat Intelligence), virus protection and spyware protection filtering engine, and SSL decryption into one unified threat management (UTM) security appliance, designed to offer centralized perimeter security.

You can use the Control Center to manage your firewalls in various ways:

- As standalone firewalls
- As members of device groups
- As members of a cluster

The Control Center provides the following functionality for firewalls:

- Firewall addition
- Configure standalone firewalls
- Manage configured firewalls using the Control Center interface

Firewall deployment options

The internal and external network interfaces of the firewall are defined during initial configuration. However, you can configure additional interfaces to suit the needs of your network infrastructure.

The firewall can be used in any or all the following ways:

- As a gateway between your internal network and the Internet
- As a gateway between any networks with different security needs
- As a transparent firewall inside of a single network
- As a SPAN-enabled firewall to analyze traffic

Traffic is passed through the firewall by arriving on one interface and leaving on a different interface. The relationship between configured interfaces can be classified in the following ways:

- **Routed** — A firewall interface is connected to each unique network, and the firewall allows traffic to pass between the networks like a router, which enforces your security policy.
- **Transparent (bridged)** — Two firewall interfaces are connected inside of a single network and are bridged to form one transparent interface. Traffic passes through the firewall like a switch, allowing you to enforce security policy inside the network without having to re-address the network. In other words, this firewall can be placed anywhere inside of your network without having to reconfigure your network.

  Note: You can configure only one transparent interface (bridge) on each firewall.
- **Hybrid** — This consists of a single bridged interface and additional routed interfaces on one firewall. This is called *hybrid mode*.
- **SPAN** — You can enable SPAN mode on firewalls to passively analyze network traffic without disrupting the existing network.

Routed mode

In routed mode, your firewall is deployed at the intersection of multiple networks.

- The firewall is connected to each network by a network interface.
- Each firewall interface must be 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 by using the firewall's IP address as their 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.

For examples of deploying a firewall in single or multiple networks, see the *Forcepoint Sidewinder Product Guide*.

Transparent (bridged) mode

In transparent (bridged) mode, your firewall is deployed inside of a single network.

A transparent interface consists of multiple interfaces that are connected inside of the same network and that are assigned to unique zones.

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

Table 19: Standard interface

Use-defined interface name	NIC or NIC group	Zone name
external_network	em0	external
internal_network	em1	internal

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

Table 20: Transparent interface

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

When traffic attempts to cross the transparent interface (from one zone to the other), an access control rule check is performed to enforce security policy. Because hosts inside of the network are not aware that the firewall is deployed, they communicate with each other as though they were directly connected by a switch.

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

For examples of transparently enforcing security policy inside of a single subnet or transparently protecting a single network, see the *Forcepoint Sidewinder Product Guide*.

Related tasks

Create a transparent (bridged) interface on page 267

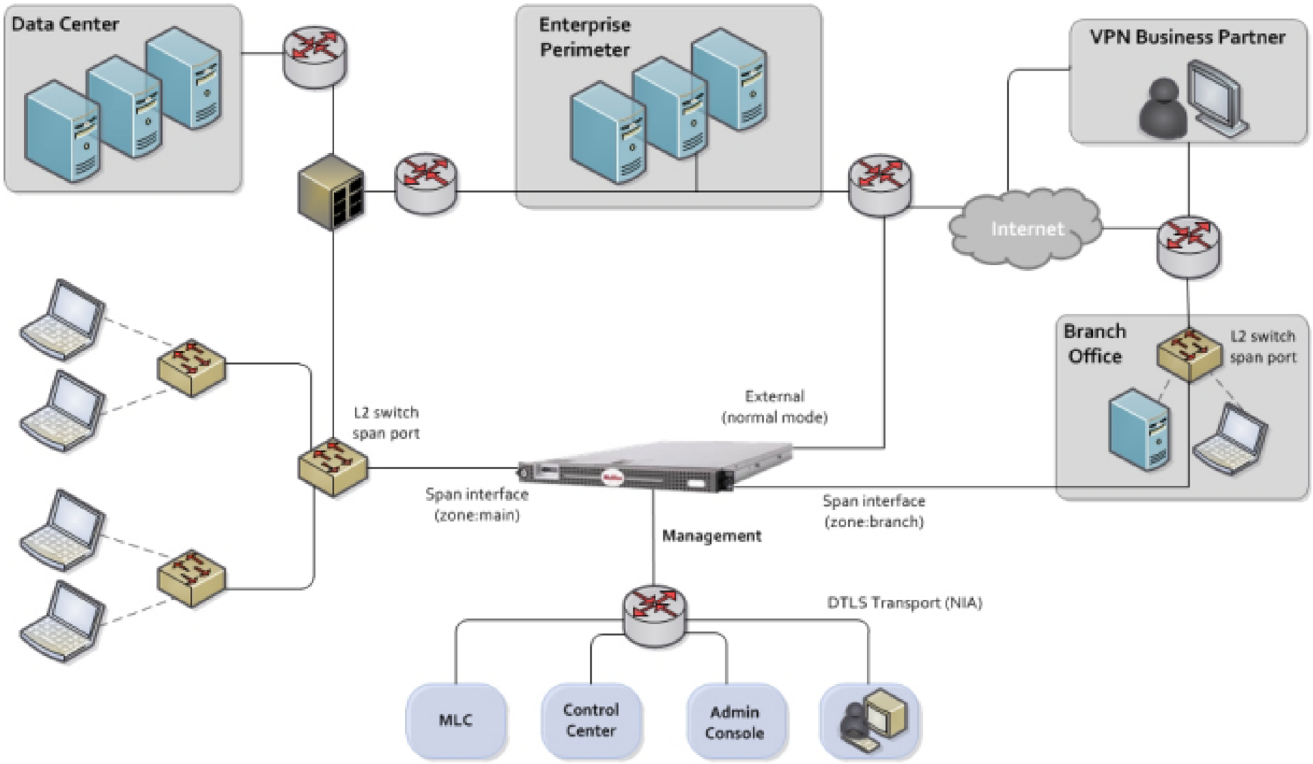
Switched Port Analyzer (SPAN) mode

Switched Port Analyzer (SPAN) mode enables Sidewinder to plug into the network and passively analyze traffic. You can evaluate Sidewinder in SPAN mode and then decide to change it to inline mode or retain it for test purposes.

Note: SPAN mode is supported only on Sidewinder 8.3.0 or later.

Sidewinder connects to the switch's SPAN port, analyzes two-way traffic, and uses output data to generate audits and reports for users like McAfee Logon Collector, Host Agent, Geo-Location, and Threats (IPS).

Figure 14: SPAN mode deployment scenario



Note: SPAN mode can co-exist with the normal mode. Firewall analyzes span traffic through the SPAN port and normal traffic from the remaining ports.

Control Center allows you to configure SPAN interfaces, zones, and rules for a selected firewall. You can apply SPAN policies across multiple firewalls.

Supported features

Firewall supports these features in SPAN mode:

- McAfee® AppPrism™
- Geo-Location
- Multiple SPAN zones
- Multiple SPAN interfaces

- Users like McAfee Logon Collector
- Display of audit data in Audit Viewer and Dashboards
- Analysis of broadcast, multicast, unicast, and VLAN traffic

Unsupported features

These features are not supported in SPAN mode:

- MTU
- NAT
- IPS
- Quality of Service (QoS) profile
- Redirect
- URL extraction
- SSL rule configuration
- VPN configuration
- McAfee GTI
- DHCP, LAGG, Bridge, PPoE, and transparent interfaces

Refer to *Forcepoint Sidewinder Product Guide* for more details on SPAN mode.

Configure SPAN mode

You can enable SPAN mode for a new interface, assign it to a zone, configure a rule, and apply the configured policy to a firewall.

Note: SPAN mode is supported only on Sidewinder 8.3.0 or later.

Create and assign a SPAN zone

A SPAN interface must be assigned only to a SPAN zone. You can create a maximum of 64 SPAN zones except any active zones that have non-SPAN interfaces.

Note: A zone is tagged as SPAN zone when it is assigned to a SPAN-enabled interface.

CAUTION: Internal, external, and heartbeat zones are reserved zones. Do not use these zones for SPAN interfaces as they might conflict with the non-SPAN interfaces.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Network Objects** node.

4) Double-click the **Zones** node.
The **Zones** window is displayed.

5) Select a firewall and the zone options for the firewall. Click **OK**.

6) Double-click the firewall.

7) In the tree, click **Interfaces**.
The **Interfaces** area is displayed.

8) In the **Firewall Interfaces** tab, select a SPAN interface row.

Tip: A SPAN interface displays the **SPAN mode enabled** column value as **Y**.

9) Click **Edit**.
The **Interface Properties** window is displayed.

10) In the **Address Configuration** area, go to the **Zone** drop-down menu and select the SPAN zone.

11) Click **OK**.

Note: You can add SPAN zones to a zone group and create multiple zone groups. A zone group can have SPAN and non-SPAN zones.

Create a SPAN interface

Enable SPAN mode for a new interface and assign it to a zone.

Note: We recommend that you create a SPAN interface instead of enabling SPAN mode on an existing interface. Exceptions are VLAN and interfaces that are not part of external, internal, and heartbeat zones.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Firewalls** node.

3) Double-click the firewall.

4) In the tree, click **Interfaces**. The **Interfaces** area is displayed.

5) In the **Firewall Interfaces** tab, click **Add**.

6) Select **Add Standard Interface**. The **Interface Properties** window is displayed.

Note: SPAN mode is not supported on transparent interfaces.

Tip: You can create a SPAN zone from this window.

7) Select the **Enable SPAN mode** checkbox. Enter details for the new SPAN interface.

Note: Some fields are disabled when SPAN mode is enabled for an interface.

8) Click **OK**.

Configure a SPAN rule

Create and configure a rule for the SPAN zone. Select the Application defense as **Default** or **connection settings**.

Before you begin

Consider these points to configure rules for the SPAN zones.

- For a SPAN rule, the source and destination zone must be the same SPAN zone. Do not use the same zone for SPAN and non-SPAN interfaces.
- A SPAN rule must be configured as the top rule (pos=1) in the rule list. If the SPAN rule is not configured on the top of the rule list, it may intersect with other rules configured with zone 'Any' and the traffic from SPAN interface may end up matching a different policy. This may not provide the expected result.
- A SPAN rule must have an action of **Allow**.
- NAT, Redirect, GTI reputation, and IPS are not supported for SPAN rules.

Configure a SPAN policy

Create and configure a policy using the SPAN zones and interfaces. Apply the configuration to single or multiple firewalls.

Firewall addition

The following methods are available to add your firewalls to the Control Center Management Server.

- Add multiple firewalls at one time

  Note: You will have to register these firewalls in a separate process.

- Add, register, and retrieve the configuration of a single firewall

Add multiple firewalls at one time

You can sign up one or more firewalls by initiating the process from the Control Center Management Server, rather than from the firewall. This process can be initiated only under specific conditions and only for specific firewalls that have been prepared to employ this option.

Before you begin

The firewalls must be configured for rapid deployment.

You can also import a prepared file for multiple firewalls to avoid manually specifying the details that are required to support this option. To use this feature, all the firewalls must have the same password.

Sign up multiple firewalls by using the **Sign Up Firewalls** window.

Note: After you complete this task, you will still have to register each firewall separately as an additional task. To add and register a single firewall in one wizard, use the **Add New Firewall Wizard**.

To add multiple firewalls at one time:

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, right-click the **Firewalls** node and select **Sign Up Firewalls**. The **Sign Up Firewalls** window is displayed.

3) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

4) Click **OK** to start the registration process. View the progress of the firewall enrollment process on the **Deployment Status** page.

Add a single firewall

After the Control Center Management Server has been installed and the firewall-specific, Control Center-enabling configurations have been made, you can begin to add new firewall objects and their associated configuration objects to the Control Center Management Server database.

You can add and register a new firewall to the Control Center by using the **Add New Firewall Wizard**. You can also retrieve the configuration from the firewall.
To use this wizard, the Control Center must be able to have SSH access to the firewall. You must configure this SSH access on the firewall. Use the Forcepoint Sidewinder Admin Console to enable the SSH access control rule on this firewall for external sources and destinations. After you save this change, you can come back to the Control Center Client application and run the **Add New Firewall Wizard**.

Creating firewall objects is a two-part process:

1) All types of firewall objects that represent physical devices in your configuration must be identified by providing basic information.

2) All the firewall-specific configuration information must be created or retrieved for each firewall.

Both of these parts can be performed in the **Add New Firewall Wizard**. You can use the **Add New Firewall Wizard** as described in the following examples:

- You have already added several firewalls by using the **Sign Up Firewalls** window. Now you need to retrieve their configurations. Perform a retrieve for each firewall individually with this wizard.
- If a single firewall is not registered with the Control Center, you can add it, register it to Control Center, and retrieve its configuration—all in one step.
- If a single firewall has already been registered with the Control Center, you can add it and retrieve its configuration.

Note: If a firewall has already been added to and registered with the Control Center Management Server, you can retrieve its configuration by using the **Firewall Retrieval Options** window.

Steps

1) In the navigation bar, select **Policy**.

2) To display the **Add New Firewall Wizard**:
   - In the **Policy** tree, double-click the **Firewalls** node.
   - Right-click the **Firewalls** node and select **Add Object**.

   Tip: For option descriptions, press **F1**.

3) To begin the process of adding the firewall to the list of firewalls in the **Policy** tree, complete the information on the **Firewall Connection Information** page and click **Next**. The **Firewall Registration Information** page is displayed.

4) Select an option to register the firewall with the Control Center Management Server.

   To skip the registration process, on the **Firewall Registration Information** page, click **Next**. The **Retrieval of the firewall into Control Center** page is displayed. Skip to Step 7.

   To register this firewall with the Control Center Management Server:

   a) On the **Firewall Registration Information** page, select the **Register the firewall with this Management Server** checkbox.

   b) Click **Next**. The **Summary** page is displayed.

5) On the **Summary** page, verify the information that you have configured. If it is correct, click **Register**; if not, correct any problems. The **Registration Status** page is displayed.

6) On the **Registration Status** page, view the progress of the firewall registration. After it successfully completes, click **Next**.

7) To retrieve items and categories from the firewall into Control Center, on the **Retrieval of the Firewall into Control Center** page, select the items and categories to be retrieved and click **Finish**. These objects are retrieved and the firewall is displayed in the list of firewalls in the **Policy** tree.

Configure the firewall by using the Firewall window

The **Firewall** window is used to configure the policy settings for a firewall. After you configure these settings, you must apply them to the firewall.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Firewalls** tree, expand the **Firewalls** node.

3) Double-click the firewall object to be edited. The **Firewall** window is displayed.

4) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

5) Click **OK** to save the firewall configuration.

Result

Next, you must apply these changes to the firewall for them to take effect.

Related tasks
Apply firewall configurations on page 370

Routing on the firewall

Traffic between machines on different networks or subnets requires routing. This routing information can be input manually by using *static routes* and can be learned automatically by using *dynamic routing*.

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 firewall can participate in routing by using information from static routes, and can act as a default gateway for your network.

Each type of route is defined in a separate area of the **Firewall** window.

Static routing

For default routes, use the fields in the **Static Routing** area of the **Firewall** window to define an alternate default route and ping addresses for the default routes.

- The firewall continuously pings the default route IP address and any other ping addresses that you define in this area.

- If all the configured ping addresses fail, the alternate default route becomes the acting default route.
- Reset the primary default route when it is active again by selecting the **Revert default gateway to the primary default gateway** option in the **Control Actions** field in the **Device Control** window.

Dynamic routing

Dynamic routing is performed by using a dynamic routing application along with one of several routing protocols.

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

The firewall implementation of the BGP, OSPF, and RIP protocols and corresponding server processes is based on the Quagga implementation. The firewall implementation of PIM-SM is based on the XORP (eXtensible Open Router Platform) implementation.

Each routing application is associated with a configuration file that contains all the information required for configuring dynamic routing. Use the Dynamic Routing area to select a configuration and to edit the associated configuration file.

> **Note:** Editing configuration files associated with dynamic routing protocols and applications requires advanced knowledge.
> If you edit one of the Quagga configuration files that is accessible from this area and apply the configuration to the firewall, the modified configuration will be validated before the information from the Control Center can be applied to the firewall.
>
> If you edit the XORP configuration file, the modified file will be validated before the XORP implementation is modified. If the configuration is invalid, the XORP implementation will continue to use its older configuration.
>
> For the Quagga implementations, consult the documentation available at http://www.nongnu.org/quagga/docs.html

For dynamic routes, you can select and edit configurations for several different protocols on the **Dynamic Routing** area of the **Firewall** window.

Benefits of dynamic routing

Dynamic routing protocols facilitate the exchange of routing information between routers. Routers acquire the network topology by communicating and updating the routing tables accordingly.

The benefits of dynamic routing include the following:

- You do not have to manually configure and maintain routing information.
- The network can quickly adapt to changes such as the addition, removal, or failure of network devices.
- Network performance improves because routers select the best path for connections between network devices.

See the *Forcepoint Sidewinder Product Guide* for more information about dynamic routing.

Configure dynamic routing for firewalls on Crossbeam X-Series Platforms

Modify the dynamic routing configuration file from the Control Center Client application.

Control Center version 5.2.1 and later support dynamic routing for managed firewalls on Crossbeam X-Series platforms.

Note: Editing configuration files associated with dynamic routing protocols and applications requires advanced knowledge.

Steps

1) In the navigation bar, click **Policy**.

2) In the Firewalls tree, click the **Firewalls** node. Double-click the firewall to configure dynamic routing for.
   The Firewall window is displayed.

3) In the tree on the left, click **Dynamic Routing**.
   The Dynamic Routing area is displayed.

   Note: For option descriptions, press **F1**.

4) From the drop-down list, select the appropriate dynamic routing configuration file.
   The configuration file appears.

5) Modify the configuration file as needed.

6) Click **OK**.

Result

The configuration file is updated the next time you apply changes to the firewall.

Apply objects to one or more firewalls

You can apply objects to a firewall in different ways in the Control Center Client application.

Use the *single object drag method* in the **Policy** tree of the **Policy** icon to drag a single object to one firewall at a time.

You can also use the *multiple object application method* to simultaneously add multiple objects to multiple firewalls.

The following object types can be used in either method:

- Global Settings

  Note: If global settings are applied to a firewall, either by dragging this object or by using the **Firewalls** window, the only other object that you can apply to this firewall is another global settings object. Otherwise, you must deselect the **Apply Global Settings** checkbox in the **Settings** area of the **Firewall** window.

- Retrieved Audit Export configuration files
- Syslog Server settings
- Network Defenses
- Servers and Service Settings
- IPS Signature Browser settings
- McAfee Global Threat Intelligence
- Virus Scan
- Scheduled Jobs
- Third-Party Updates
- Package Load

Apply objects to a firewall by dragging them to the firewall

As a shortcut to configuring objects directly in the **Firewall** window, you can add or change object values in the **Firewall** window without having to open that window in the **Policy** icon. The object that you drag from the **Firewall Settings** tab to the firewall will overwrite the existing value in the **Firewall** window.

Although this is very useful for editing objects for the firewall, you should initially configure your firewall by using the **Firewall** window.

The following procedure is an example of this function:

Steps

1) In the **Policy** tree, make sure that the target firewall node is displayed in the tree.

2) Make sure that the **Firewall Settings** tab is displayed.

3) Make sure that the object node to be used is displayed in its object tree on the **Firewall Settings** tab. For this example, make sure that the **Default Network Defenses** object is visible in the **Network Defenses** node.

4) Drag the object (in this example, the **Default Network Defenses** object) to the firewall. You can double-check this change by opening the **Firewall** window and viewing the object field in the **Settings** area.

5) Apply your changes to push the object change to the firewall.

Apply objects to multiple firewalls

You can select multiple firewalls as the target of one object by using the **Apply on Firewalls** window.

This is an alternative to dragging one object to apply to one firewall.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Select the node of the object type that you are going to apply so that this object list is expanded to display all its objects.

4) Right-click the object that you want to apply and select **Apply on**. The **Apply on Firewalls** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Select your firewalls and click **OK**. The object or objects are applied to the selected firewall or firewalls.

   Note: You must still apply these changes to the firewall.

Manage configured firewalls using the Control Center interface

The following topics provide more detailed information about managing your configured firewalls.

Firewall components (objects)

Firewall components or objects are part of the firewall configuration. Although you can add a firewall to the list of firewalls in the **Policy** tree, a firewall is not registered in the Control Center Management Server database until its components are retrieved from the firewall.

The list of the components that can be retrieved is firewall-specific.

Each component has an associated checkbox. Select the checkbox to retrieve the associated components. If you select certain components, other related or subordinate components will automatically be selected. For example, if the **Firewall Dialog** (window) **Information** component is selected, the **Firewall Interfaces**, **Firewall Certificates**, **CA Certificates**, and **Authentication Services** components are also selected for the firewall.

The table illustrates the information that is retrieved by component type

Table 21: Firewall components and retrieved information

Component	Information
Firewall Interfaces	• Firewalls • Clusters • Cluster members • Zone groups • Zone indexes • Zones • Interface versions • Interfaces • Cluster interfaces • Networks • Filter services • Proxy services • Service groups • QoS profiles • NICs • NIC groups
Firewall Dialog Information	• Firewalls • Clusters • Cluster members • CA certificates • CA certificate groups • Firewall certificates • SSH server keys • Local certificate authorities • Address ranges • Domains • Geo-Location endpoints • Endpoint group • Hosts • Networks • Netmap endpoints • Filter services • Proxy services • Service group • Daemon servers • Dynamic application groups • Static application groups

Component	Information
Firewall Dialog Information (continued)	• Custom applications • Standard applications • Application categories • DNS zones • Cron Tab sets • Package load • Package schedule • Scheduled updates • Scheduled backup • QoS profiles • IPS raw signature status • Global Threat Intelligence • Audit export • Audit filters • Net defense audits • Syslog reporter • Password authenticators • Passport authenticators • RADIUS authenticators • Safeword authenticators • Windows authenticators • IPlanet authenticators • Active Directory authenticators • OpenLDAP authenticators • Custom LDAP authenticators • External groups • CAC Authenticators • SmartFilter Categories • SmartFilter Policies • SmartFilter Settings
Firewall License	• Firewall features • Firewall hardware keys • Firewall license • Default firewall license
Firewall Certificates	• Firewall certificates • SSH server keys • Local certificate authorities

Component	Information
CA Certificates	- CA certificates - CA certificate groups - Local certificate authorities
Network Objects	- Zone groups - Zone indexes - Zones - Address ranges - Domains - Geo-Location endpoints - Endpoint groups - Hosts - Networks - Interface version - Interfaces - Cluster interfaces - Networks - Netmap endpoints
Services or Applications	- Filter services - Proxy services - Service groups - Daemon servers - Dynamic application groups - Static application groups - Custom applications - Standard applications - Application categories
Users	- Administrators - Users - User groups - External groups - CAC authenticators

Component	Information
Miscellaneous	• Networks • DNS zones • Cron Tab sets • Package load • Package schedule • Scheduled updates • Scheduled backups • Time periods • QoS profiles • NICs • NIC groups • SmartFilter categories
Application Defenses	• Application Defense groups • Citrix Application Defenses • FTP Application Defenses • Generic Application Defenses • H323 Application Defenses • HTTP Application Defenses • HTTPS Application Defenses • IIOP Application Defenses • Mail (Sendmail) Application Defenses • Mail (SMTP proxy) Application Defenses • MSSQL Application Defenses • ORACLE Application Defenses • Packet Filter • SIP Application Defenses • SNMP Application Defenses • SOCKS Application Defenses • SSH Application Defenses • T120 Application Defenses • SmartFilter categories • SmartFilter policies • SmartFilter settings
Content Scanning	• Header spam filters • Host spam filters • Virus scans • SmartFilter categories • SmartFilter policies • SmartFilter settings

Component	Information
IPS Signature Categories and Class Types	• IPS actions • IPS signatures • Raw IPS signature statuses • Static IPS data
GTI	• McAfee Global Threat Intelligence
IPS Objects	• IPS actions • IPS signatures • Raw IPS signature statuses • Static IPS data
VPN	• VPN communities • VPN peers • IKE strategies • IPSec strategies • IKE proposals • IPSec proposals • VPN client configurations • VPN identities • VPN bypasses
Audits and Alerts	• Email accounts • Host blackholes • Audit export • Audit filters • Net defense audits • Responses • Syslog reporters
Authentication Services	• Password authenticators • Passport authenticators • RADIUS authenticators • Safeword authenticators • Windows authenticators • IPlanet authenticators • Active Directory authenticators • OpenLDAP authenticators • Custom LDAP authenticators • External groups • CAC authenticators

Component	Information
Rules	• Users • User groups • Time periods • Packet filter rules • Rules • URL rules • SSL rules

Retrieve firewall components

You must be able to retrieve objects from a firewall as part of its registration process on the Control Center Management Server.

You can do this in several different ways, depending on the version of firewall that you are retrieving the objects from. However, the retrieval process is the same for all of them.

- [Available for firewall version 8.1.0 or later] The **Add New Firewall Wizard** has component retrieval included as part of the registration process. You can retrieve objects at that time.

  > **Note:** If you decide to skip that part of the wizard, you can go to the **Firewall Retrieval Options** window to do it at a later time.

- The **Firewall Retrieval Options** window can be used to retrieve objects from any firewall.

  > **Note:** If you have already retrieved objects in the **Add Firewall Object Wizard**, retrieving again will overwrite your initial settings.

Steps

1) Navigate to the list of objects to retrieve.
   - If you are retrieving objects from a new firewall:
     1) In the navigation bar, select **Policy**.
     2) In the **Policy** tree, right-click the **Firewalls** node and select **Add Object**. The **Add New Firewall Wizard** appears.
     3) Specify the required information and continue to the **Firewall Registration Information** page.
   - If you are retrieving objects from a firewall that is already added to Control Center:
     1) In the navigation bar, select **Policy**.
     2) In the **Policy** tree, expand the **Firewalls** node.

3) Right-click the firewall object and select **Retrieve Firewall Objects...** The **Firewall Retrieval Options** window appears.

> **Tip:** For option descriptions, press **F1**.

2) In the list of retrieval items, select the items to be retrieved.

> **Tip:** Right-click the column heading to select all or deselect all fields.

3) Retrieve the objects.

In the **Add New Firewall Wizard**:

a) Click **Next**. The **Summary** page is displayed.

b) Click **Next** to continue with the retrieval and registration.

c) Complete the wizard. Afterwards, the firewall will be successfully registered to the Control Center Management Server.

In the **Firewall Retrieval Options** window:

a) Click **OK**. A confirmation message is displayed.

b) Click **Yes**. The objects are retrieved from the firewall.

Related concepts

Firewall components (objects) on page 252

View object use

You can select an object and then display all the other objects that are used or referenced by this object.

This is helpful when you attempt to delete an object, only to receive a message that it is being referenced by another object. The Usage of *object_name* Object window is displayed automatically if you attempt to delete an object that is being used in a firewall configuration. You can view the referenced objects and edit the references to them so that you can then delete the object. You can also export this data to a file in comma-delimited (CSV) format.

Steps

1) In the navigation bar, select **Policy**.

2) In the Policy tree, expand the **Firewalls** node.

3) Right-click the firewall and select **Show Usage**. The Usage of *object_name* Object window is displayed.

> **Tip:** You can also click **Show Usage** on the search results of a show usage.

4) You can edit objects in the tree by expanding the nodes and double-clicking the individual objects. The window for that object is displayed, where you can edit and save the values.

5) [Optional] Export this data to a comma-delimited (.csv) file.

Tip: For other option descriptions, press **F1**.

6) Click **Close** to close this window.

Manage (sort) the view of your configured firewalls

The Control Center Client application presents your firewalls in the **Policy** tree in a default display order. You can change this order in the **Firewall Sorting** window.

You can select the firewall characteristics and the order of consideration of those characteristics to determine the way that the firewalls are displayed by using a standard selection list.

The available sort characteristics for display configuration are:

- **Location** — The user-defined location information
- **Contact** — The user-defined contact information that is associated with a firewall
- **Any user-defined category/value pair** — The category/value pair that is defined on the firewall or in the **General** area of the **Firewall** window

By careful management of the location information, contact information, and user-defined categories that are associated with each firewall, you can create a powerful and effective firewall-sorting plan to manage large numbers of firewalls.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Firewalls** node or the **Clusters** node.

3) Right-click a firewall or cluster node and select **Firewall Sorting**. The **Firewall Sorting** window is displayed.

Tip: For option descriptions, press **F1**.

4) Configure the fields on this window as needed.

5) Click **OK** to save your changes. The firewalls or clusters should be rearranged in their respective nodes based on your changes.

Delete firewall objects

You can remove firewall objects from the list of firewalls in the **Policy** tree.

This is normally a right-click menu option. However, if there are any dependencies on the targeted firewall, the **Delete Firewall** window is displayed. You can view the dependences and determine the way that you will proceed with this firewall. Certain dependencies, if left unresolved, will prohibit the firewall from being deleted.

Steps

1) In the navigation bar, select **Policy**.

2) In the Policy tree, click the **Firewalls** node.

3) To delete the firewall:

   - Right-click a firewall node and select **Remove Object(s)**.
   - Select a firewall node and press **Delete**. A confirmation message is displayed. Click **Yes** to continue.

   The **Delete Firewall** window is displayed *only* if there are dependent objects that are associated with this firewall object.

4) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

5) Click **Delete Firewall** to delete the firewall object.

6) Click **OK** in the confirmation message.

Manage configured firewalls using a Secure Shell interface

You can use a Secure Shell (SSH) interface to locally manage some components of the Forcepoint Sidewinder or the Forcepoint Sidewinder on Crossbeam X-Series Platforms (firewall cluster on X-Series Platform).

Security for the connection is enforced through the use of encryption and authentication.

Secure Shell (SSH) relies on an application-level, client-server model. An SSH client remotely accesses a system that is running an SSH server process by using the SSH application-level protocol. The SSH client can invoke a standard UNIX® operating system shell, a command line application, or an X Window System™ session on the remote SSH server. Note that, because the client can open a UNIX shell or X Window System session on the server, it is implied that the SSH server can run only on a UNIX system. The SSH client can be run from any operating system to which it can be ported.

You can access the native firewall interface of a firewall system that is managed by the Control Center by using the Secure Shell window. In the case of the firewall on X-Series Platform, certain interfaces can be managed only locally.

You can specify the connection parameters in the Secure Shell window.

Before you can establish a Secure Shell connection to the firewall, you must have performed the following prerequisites:

- Install an SSH client on the Forcepoint Sidewinder Control Center Client platform.
- The access control rule for SSH is activated.
- [For the firewall on X-Series Platform only] You have specified the IP address or URL of this firewall in the **Hostname/IP address** field in the **Appliance Address** area of the **General** area on the **Cluster** window.

To access the Secure Shell window:

Steps

1) In the navigation bar, select **Policy**.

2) In the Policy tree, expand the **Firewalls** node or the **Clusters** node.

3) Right-click a firewall or cluster node and select **Launch Secure Shell**. The **Secure Shell** window is displayed.

   Tip: For option descriptions, press **F1**.

4) Make sure that the path is correct in the **SSH Client** field.

5) Specify any command line options in the **Command Line Options** field.

6) To append the management address or URL of the firewall to the value that you specified in the **Command Line Options** field, select the **Append management address (ip_address or URL) to options** checkbox.

7) [For the firewall on X-Series Platform only] To append the firewall management URL or IP address value to the value in the **Command Line Options** field, select the **Append appliance address (address) to options** checkbox.

8) Click **Connect** to connect to the Secure Shell interface.

How Control Center counts ping failures

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.

Ping failures and successes

If you set the allowed number of failures to **3**, the following table demonstrates the way that successful and failed pings are counted to determine the failover.

Table 22: Ping failover count example

Ping result:	failure	success	success	failure	failure	success	failure	failure	*Failover event occurs*
Failure total:	1	0	0	1	2	1	2	3	

Interfaces and NICs

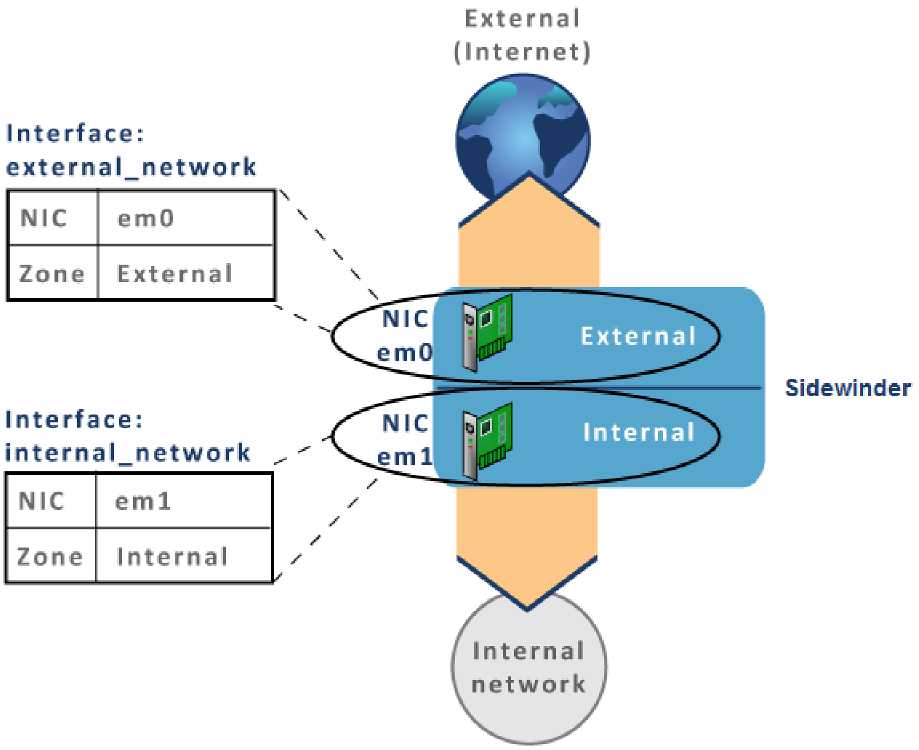
An interface on the Control Center is a logical representation of a network connection.

The interface configuration includes many settings, one of which is the associated hardware device that connects the firewall to this network. The network interface card (NIC) or NIC group serves as the hardware device.

As shown in the following figure, NICs and zones are two of many different attributes that define the interface.

Because of the relationship between interfaces and NICs, you can easily move your network configuration to different network hardware by assigning a different NIC to an interface.

Figure 15: Relationship between interfaces, NICs, and zones



Interface types

You can create and configure the following different types of interfaces on the **Firewall Interface** window.

- Standard — A standard interface is a single interface that has a static IP address assigned to it.
- VLAN — Use a VLAN interface as a virtual interface to segment 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.
  - 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`*
- DHCP — Use a Dynamic Host Configuration Protocol (DHCP) interface to centrally manage IP addresses within your network.
  - Only one DHCP interface can be enabled at a time.
  - You can enter IPv6 addresses on an interface that is using DCHP for IPv4 addresses.
  - DHCP interfaces are not allowed on an HA cluster.
- Transparent — A transparent interface consists of two bridged interfaces. Use a transparent interface to separate a single Ethernet segment into two zones. You can enforce security policy on traffic that passes through the transparent interface without re-addressing the network around the firewall.
  When you configure a transparent interface, you cannot enable or configure the following features and objects:
  - 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
- High Availability (HA) — If the firewall is part of an HA cluster, you will need to define both the cluster ID address and the original (primary) IP address of the interface before joining the HA cluster. In each HA cluster, three interfaces should have a cluster IP address: the heartbeat zone and one interface for each cluster member. You can create additional interfaces for private or management purposes without assigning a cluster IP address to them.

  Note: You can use IPv6 addresses in an HA cluster for 8.2.0 and later firewalls.

Configure interface types

You can create and configure different interface types by using the following procedures.

Note: You cannot create or modify any type of interface on a firewall cluster node on X-Series Platform or on a cluster member node on X-Series Platform.

Create a standard interface

You can create a single interface with a static IP address assigned to it.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Firewalls** tree, click the **Firewalls** node. Double-click the firewall to configure the transparent interface for. The **Firewall** window is displayed.

3) In the tree on the left, click **Interfaces**. The **Interfaces** area is displayed.

> **Tip:** For option descriptions, press **F1**.

4) Add a new interface row to the table by clicking **Add** at the far right of this area. A new row is added to the table.

- The value in the **Zone** field is **<None>**.
- The value in the **NIC/NIC Group** field is also **<None>**.

5) Specify values in all the fields. In the **Type** field, select **Standard**.

6) Click **Advanced** to display the **Firewall Interface** window, where you can configure additional settings. In this window, you can configure alias addresses, MTU size, and optional IPv6 values.

7) Click **OK** to save your changes in the **Firewall Interface** window.

Create a DHCP interface

You can create a Dynamic Host Configuration Protocol (DHCP) interface to centrally manage IP addresses within your network.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Firewalls** tree, click the **Firewalls** node. Double-click the firewall to configure the transparent interface for. The **Firewall** window is displayed.

3) In the tree on the left, click **Interfaces**. The **Interfaces** area is displayed.

> **Tip:** For option descriptions, press **F1**.

4) Add a new interface row to the table by clicking **Add** at the far right of this area. A new row is added to the table.

- The value in the **Zone** field is **<None>**.
- The value in the **NIC/NIC Group** field is also **<None>**.

5) Specify values in the fields. In the **Type** field, select **DHCP**. The following changes occur in the table:

   a) The value in the **IP address** field changes to **DHCP** and is read-only.

   b) The value in the **VLAN ID** field is read-only.

   c) The value in the **Zone** field changes to **external** and is read-only.

6) Click **Advanced** to display the **Firewall Interface** window, where you can configure MTU size, a Quality of Service profile, and you can enable IPv6 on the interface.

7) Click **OK** to save your changes in the **Firewall Interface** window.

Create a VLAN interface

You can create a virtual interface to divide a LAN into different broadcast domains, regardless of their 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.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Firewalls** tree, click the **Firewalls** node. Double-click the firewall to configure the transparent interface for. The **Firewall** window is displayed.

3) In the tree on the left, click **Interfaces**. The **Interfaces** area is displayed.

   Tip: For option descriptions, press **F1**.

4) Add a new interface row to the table by clicking **Add** at the far right of this area. A new row is added to the table.

   - The value in the **Zone** field is **<None>**.
   - The value in the **NIC/NIC Group** field is also **<None>**.

5) Specify values in all the fields. In the **Type** field, select **VLAN**. The **VLAN ID** column is available and defaults to **2**.

6) Specify a numeric ID for this VLAN.

7) Click **Advanced** to display the **Firewall Interface** window, where you can configure additional settings. In this window, you can configure alias addresses, MTU size, and optional IPv6 values.

8) Click **OK** to save your changes in the **Firewall Interface** window.

Transparent (bridged) interface

A transparent interface consists of two or more bridge member interfaces.

You can use a transparent interface to separate a single network into two zones. You can enforce security policy on traffic that passes through your firewall's transparent interface without having to re-address the network around the firewall.

Note: This function is available only for firewall versions 7.0.1.02 or later. It is not available for High Availability clusters.

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

Table 23: Standard interface

User-defined interface name	NIC or NIC group	Zone name
external_network	em0	external

User-defined interface name	NIC or NIC group	Zone name
internal_network	em1	internal

The following table shows a transparent interface that has been configured by using the default interfaces. Note that bridge0 consists of two bridge member interfaces: em0 and em1.

Table 24: Transparent interface

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

If you configure a transparent interface, you cannot enable or configure any of the following functions:

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

Related tasks
Create a transparent (bridged) interface on page 267

Create a transparent (bridged) interface

You can enforce security policy on traffic that passes through the transparent interface on your firewall without re-addressing the network around the firewall.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Firewalls** tree, click the **Firewalls** node. Double-click the firewall to configure the transparent interface for. The **Firewall** window is displayed.

3) In the tree on the left, click **Interfaces**. The **Interfaces** area is displayed.

   Tip: For option descriptions, press **F1**.

4) Click **Add** and select **Add Transparent Interface**.

5) Specify values in the fields.

6) In the **Bridged interfaces** area, select the two interfaces to use for this transparent interface and modify their settings.

7) Click **Advanced** to configure additional settings. In this window, you can configure interface ID and ARP table cache size.

8) Click **OK** to save your changes.

Related concepts

Transparent (bridged) interface on page 266

Manage interface configurations

Create or modify configuration information for a network interface on a firewall or on a cluster member in the **Firewall Interface** window.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, for firewalls, expand the **Firewalls** node.

   For cluster members, expand the **Clusters** node and then select a cluster node.

3) Double-click a firewall or cluster member in the tree or right-click the object and select **Edit Member Settings** or **Edit Cluster Settings**. For firewalls, the **Firewall** window for the selected firewall is displayed.

   For cluster members, the **Firewall Cluster Member** window for the selected cluster member is displayed.

4) In the tree on the left, select the **Interfaces** node. The **Interfaces** area is displayed.

5) Click **Advanced**. The **Firewall Interface** window is displayed.

   Tip: For option descriptions, press **F1**.

6) Configure the fields on this window as needed.

7) Click **OK** to save this interface.

Related tasks

Convert network objects in access control rules for the IPv6 protocol on page 308

NIC groups

For version 7.x firewalls, you can bundle two NICs into a NIC group as a redundant NIC group for backup purposes.

For version 8.0.0 firewalls or later, in addition to redundant NIC groups, you can bundle two or more NICs into an aggregate group by using link aggregation (LAGG).

The following specifications apply to NIC groups:

- The same media capabilities must be enabled on all NICs in a group.
- 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 can consist of up to 32 NICs. We recommend the following configuration:
  - **Aggregate** — [Available only for 8.0.0 firewalls or later] You can have as many NICs per aggregate group as you need. Results might vary, depending on your specific hardware.
  - **Redundant** — You can have two or more NICs per redundant group for version 8.0.0 firewalls or later. You can have only two NICs per redundant group for version 7.x firewalls.
- A total of up to 63 NICs and NIC groups can be configured on one firewall.

You can use aggregate and redundant groups on a standard, VLAN, DHCP, or transparent interface.

Related concepts
Aggregate NIC groups on page 269
Redundant NIC groups on page 270

Aggregate NIC groups

An aggregate group uses Link Aggregation Control (LACP) and Marker protocols as defined by IEEE 802.1AX (formerly known as IEEE 802.3ad).

Note: Aggregate groups are available for version 8.0.0 firewalls or later.

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 by using crossover cables.

An aggregate group consists of a primary NIC and one or more peer NICs. All the peer NICs in this group inherit the MAC address and MTU of the primary NIC. The primary NIC and all the 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 increased bandwidth.

In an aggregate group, the available bandwidth does not increase for a single conversation. To maintain packet order, all the packets that are associated with a conversation are transmitted on the same link. 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 that 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 by using only the NICs in the group that share the highest bandwidth. All active NICs in the aggregate group must 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 those NICs that are operating at the highest speed and at full duplex are selected to pass traffic.

When the firewall determines the 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

An aggregate group is a good choice if you anticipate that many different users and sessions will be connecting to many different destinations on an interface.

Redundant NIC groups

A redundant group consists of one primary NIC and one standby NIC (for version 7.x firewalls only) or one primary and one or more standby NICs (for version 8.0.0 firewalls or later).

The main purpose of a redundant group is to provide increased availability. The primary NIC passes all the traffic. If the primary NIC fails (for example, disconnects), the 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.

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 the NIC that is actively passing traffic. The firewall 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.

Create NIC groups

You can create a redundant NIC group with one primary and one or more standby NICs or you can create an aggregate NIC group with one primary NIC and one or more peer NICs.

You can create NIC groups in the **NIC Group** window.

Note: There are differences between the version 7.x firewall version of this window and the version 8.0.0 or later version. Make sure that you have selected the correct version-specific Help topic.

Steps

1) In the navigation bar, select **Policy.**

2) In the **Policy** tree, expand the **Firewalls** node.

3) Double-click a firewall. The **Firewall** window is displayed.

4) In the tree on the left, select the **Interfaces** node and then click the **NICs/NIC Groups** tab. The **NICs/NIC Groups** tab is displayed.

5) At the bottom of the tab, click **Add**. The **NIC Group** window is displayed.

   Tip: For option descriptions, press **F1**.

6) Configure the fields on this window as needed.

7) Click **OK** to save this object.

IPv4 and IPv6 overview

Control Center supports both IPv4 and IPv6 addresses on the firewall, which allows you to integrate with more networks.

IPv6 support also provides access to larger blocks of routable addresses.

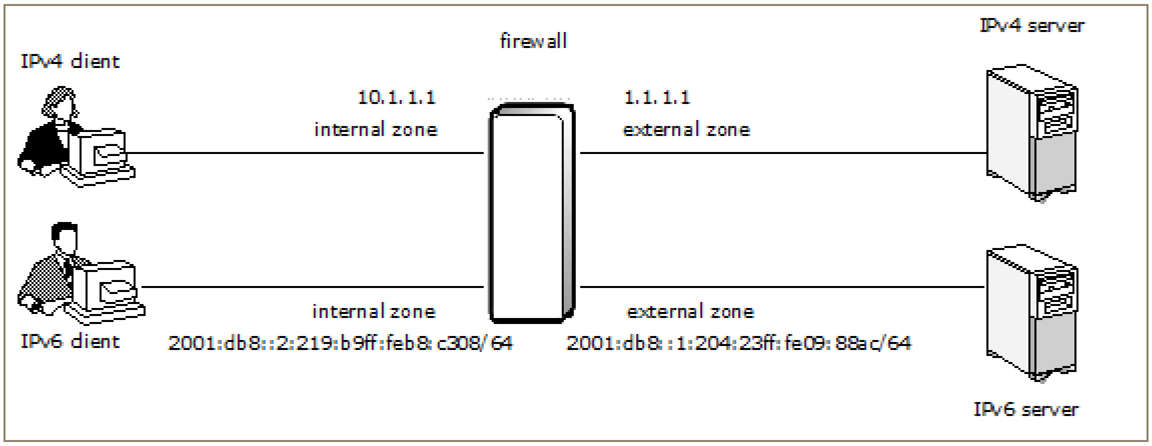
The following connection types are supported:

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

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

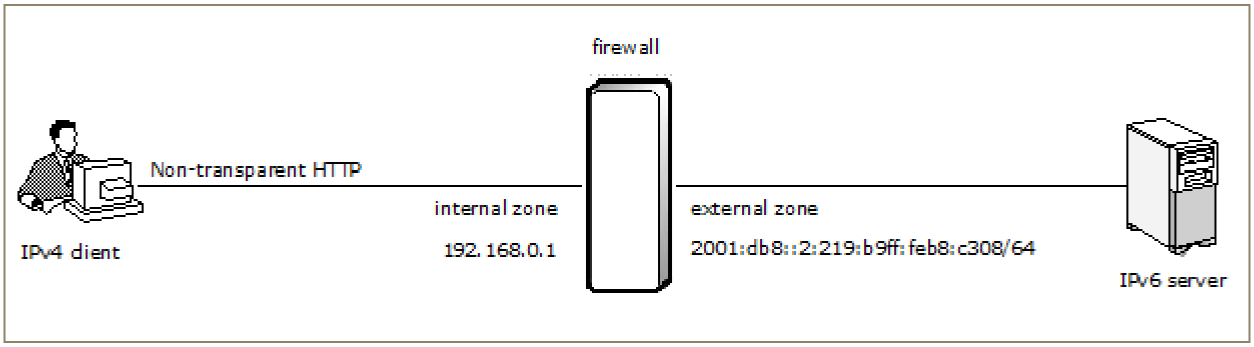
The firewall can pass both types of traffic by using dual stack architecture.

Figure 16: Dual stack architecture



You can also configure the firewall 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 17: IPv4-to-IPv6 translation



IPv6 support by feature

The following table lists IPv4 and IPv6 support by feature.

Table 25: IPv6 support by feature

Feature	IPv4 only	IPv4 and IPv6
Administration methods	• SmartFilter Administration Console • Telnet	• Admin Console • SSH

Feature	IPv4 only	IPv4 and IPv6
Applications	• Citrix Browser • Citrix-ICA • DNS • H.323 • iiop • MSSQL • Oracle • RealMedia • rlogin • RSH • RTSP • SIP • SMTP • SOCKS • Sun RPC • T120 • Telnet **Tip:** To allow these applications over IPv6, use a generic application on the appropriate port(s).	All other applications
Application Defenses	All Application Defenses except HTTP and Generic (settings ignored for IPv6)	• HTTP • Generic
Authentication (client connection to firewall)		All methods
Authentication (firewall connection to authentication server)	All remote authentication server types, including passive authentication (MLC)	Local methods only: • Password • Active Passport
Content inspection	McAfee Global Threat Intelligence	IPS
Dynamic routing	• RIP • PIM-SM	• BGP • OSPFv6
High Availability	Yes	No
Inter-product communication	• Control Center • McAfee Logon Collector • Firewall Syslog	None (can process data that contains IPv6, but cannot connect by using IPv6)
Packet filters	None	All

Feature	IPv4 only	IPv4 and IPv6
Proxies	All proxies except HTTP, TCP, and UDP	• HTTP • TCP • UDP
Servers	• DHCP Relay • sendmail	BIND (no Admin Console support for IPv6)
SmartFilter	SmartFilter Admin Console (cannot manage over IPv6 connection or filter IPv6 traffic)	Locally managed SmartFilter (Sidewinder Admin Console connection must be IPv4)
VPN (ISAKMP)	• All VPN modes except gateway-to-gateway • Client address pools	Gateway-to-gateway mode

Enable IPv6 and create IPv6 addresses on a firewall

You can create IPv6 addresses on a firewall interface. But first, you must enable IPv6 on that interface.

Perform these tasks on the **Firewall Interface** window.

Steps

1) Navigate to the firewall that you are configuring IPv6 addresses for.
    a) In the navigation area, select **Policy**.
    b) In the **Policy** tree, expand the **Firewalls** node.
    c) Double-click the firewall that you want to configure IPv6 addresses for. The **Firewall** window is displayed.
    d) In the tree on the left, select **Interfaces**. The **Firewall Interfaces** tab of the Interfaces area is displayed.
2) Select **Enable IPv6** for this interface.

3) In the **IPv6 stateless auto address configuration** area, select the configuration type. The following options are available:

   - **Static** — When selected, the interface is assigned the link-local address plus any static addresses that you specify. The link-local address is automatically created whenever an interface becomes enabled.
   - **Router mode** — When selected, the interface is assigned the link-local address plus any static addresses that you specify. 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.
   - **Host mode** — When selected, the interface is assigned the link-local address plus any static addresses that you specify. It is also assigned auto-configured addresses derived by combining any prefixes that are received in router advertisements with the interface ID.

   CAUTION: Host mode and router mode should be used only if you want to use auto-configuration. If you use these modes, unexpected results can occur, such as the following examples:

   - A firewall with an interface that is configured in host mode can automatically add new IPv6 addresses to the interface that the user might not expect.
   - A firewall with an interface that is configured in router mode with static IPv6 addresses can, if the rtadvd.conf file is not modified, 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.

4) Type an IPv6 address by specifying the address and mask length (in the **Prefix** column). Repeat as needed.

5) [Optional] You can specify an interface ID to replace the default ID.

6) Configure the other options on this window as needed.

7) Click **OK** to save this interface.

Configure transparent domain name system (DNS) server objects

The domain name system (DNS) is a service that translates host names to IP addresses, and IP addresses into host names. DNS is necessary because, although computers use a numeric addressing scheme to communicate with each other, most users prefer to address computers by name. DNS acts as the translator, matching computer names with their IP addresses.

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. The Forcepoint Sidewinder provides the additional option to host the DNS server directly on the firewall, eliminating the need for an additional computer.

There are two main DNS configurations:

- **Transparent DNS** — Transparent DNS is designed for simple DNS configurations. The DNS server is on a separate computer, and DNS requests are proxied through the firewall. This is the default DNS configuration for a newly installed Forcepoint Sidewinder.

- **Firewall-hosted DNS** — Firewall-hosted DNS represents a more complex DNS configuration that uses the integrated Forcepoint Sidewinder DNS server.

Transparent DNS is the default configuration, created during initial configuration using the Quick Start Wizard. If you want to make changes to your existing DNS configuration, you can use one of two methods:

- **Control Center Client application** — Use the Transparent DNS Servers window to make changes.
- **Manual** — Manually edit the DNS configuration files. This should be attempted only by highly skilled DNS administrators.

If you have configured DNS to use transparent services, you can add, modify, or delete transparent name servers on the Transparent DNS Servers window.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Firewalls** node for firewalls or the **Clusters** node for clusters.

3) Double-click the firewall or cluster node that you are creating this object for. The **Firewall** window (or the **Cluster** window) is displayed.

4) Click the **DNS** node in the tree on the left. The **DNS** area is displayed.

5) Make sure that **Transparent** is the value selected in the **DNS Configuration** field and click **Add**. The **Transparent DNS Servers** window is displayed.

6) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

7) Click **OK** to save this object.

CHAPTER 20

Clusters and device groups

Contents

The Control Center provides an interface for managing Forcepoint Sidewinder High Availability (HA) clusters.

About clusters

A firewall HA cluster consists of two firewalls that are configured in a particular way for High Availability.

Control Center supports management of the following Forcepoint Sidewinder HA modes:

- **Primary/standby** — In this configuration, one firewall, the primary, actively processes traffic. The standby acts as a "hot backup." If the primary becomes unavailable, the standby takes over and assumes the role of the primary only until the primary becomes available again. When the primary does become available, a takeover event occurs.
  Use this mode if you have firewalls that do not share the same hardware configuration.
- **Load-sharing** — In this *active-active HA* configuration, two firewalls actively process traffic in a load-sharing capacity. Both firewall network interfaces maintain their unique IP address, the shared cluster address, and any aliases assigned to the cluster. The firewalls are able to coordinate traffic processing on a single shared IP address by using a multicast Ethernet address. Each connection is handled by the same firewall. The communication to coordinate load-sharing passes between firewalls on the heartbeat zone.
  Use this mode only if both firewalls have the same hardware configuration (for example, CPU speed, memory, active NICs). This mode is the recommended configuration.

  Note: You cannot create a load-sharing cluster with a firewall that has IPv6 enabled.
- **Peer-to-peer HA** — In this configuration, two firewalls are configured as standbys with the same takeover time. The first firewall to come online becomes the primary. Only the primary passes traffic. If the primary becomes unavailable, the peer, which is currently acting as the standby, takes over as the primary and remains the primary until it becomes unavailable. At that time, the other peer takes over again as the acting primary.

Certain firewall features are associated with the cluster object and are synchronized within all nodes in a cluster. Other firewall features are associated with the cluster node objects and are specific to each node.

Cluster management

Use the functionality in the Control Center **Policy** icon to manage firewall HA clusters.

The **Policy** icon accommodates management of the entire cluster and management of the particular nodes that are in the cluster. This allows a firewall security officer to perform such node-specific monitoring and control functions as running reports, shutting down the firewall, setting date and time, and licensing.

In the Control Center, an HA cluster can be viewed as a single firewall. The reason is that for most configurations, one cluster node's configuration data is a replica of the other node's configuration data. A cluster object is created for every HA cluster in the **Clusters** group in the **Firewalls** tab in the **Object** area. A cluster object expands to list all individual nodes that are part of the cluster. Individual nodes are called *cluster member node objects*. You can view cluster configuration object data by double-clicking a cluster object to display the **Cluster** window. You can view cluster member node object configuration data by double clicking a cluster member node to display the **Cluster Member** window.

Note: Cluster member node objects for clusters on X-Series Platforms can automatically appear in the list of cluster member nodes for a specific cluster. This is because cluster members for these clusters are configured directly on the appliance. When any change occurs on interfaces, transparent DNS, or cluster members, Control Center auto-retrieves this information and displays the same.
You cannot add or demote cluster member nodes from the firewall cluster on X-Series Platform in the Control Center Client application as you can with other clusters. You must go directly to the firewall cluster on X-Series Platform to add or demote cluster member nodes.

However, you can delete cluster member nodes of firewall clusters on X-Series Platforms in the Control Center Client application; you cannot do this on other clusters; you can only demote cluster members.

Features that are synchronized within a cluster

The following features are synchronized within all nodes in an HA cluster. Configuration support for these features is associated with the cluster object.

- Policy configuration (access control rule)
- Authentication
- Groups
- Proxies
- Certificate management
- Services
- System responses
- User interface access control
- Time periods
- Routing
- Configuration backup
- SmartFilter
- Network defenses
- VPN
- Firewall accounts

- Servers
- Attack responses
- Interface alias IP addresses
- UPS
- High Availability
- DNS
- Virus scanner
- Zone configuration
- Reconfigure mail (sendmail)

All cluster-related information is available in one location: the cluster object.

The following functions are performed only on the cluster object:

- Apply Configuration
- Validate Configuration
- Retrieve Firewall Objects

After a node has been added to a cluster, these functions cannot be performed on the node.

The Policy Report is the only report that can be generated on the cluster object; there are no reports specifically for cluster members.

Cluster member node features

The following features are specific to each node in a cluster. Configuration support for these features is associated with the cluster node object.

- Firewall license
- Date and time
- System shutdown
- Audit
- High Availability (local parameters)
- Reports
- Interface configuration
- Certificate management
- Reconfigure DNS
- Software updates

As indicated here, such control functions as licensing, shutting down, setting date and time, and displaying firewall status can be performed only on each node.

Cluster creation

You can create a cluster in several different ways.

You can create clusters in Control Center from one or two registered firewalls. You can also join a registered firewall to an existing cluster. The **Cluster Wizard** provides the functionality to perform both of these procedures.

Make sure that cluster requirements are met

Before you begin to configure a cluster or edit an existing cluster, make sure that the following requirements have been met.

Steps

1) Verify the following requirements for all cluster types:
   - **Version** — Both firewall objects must be the same version. Also, if the firewall is joining a single-node cluster, the version of the firewall must match the version of the existing node in the cluster object.
   - **Interfaces** — The firewall object that you are working with must have at least three enabled interfaces—internal, external, and heartbeat.
     The number of and types of interfaces must be exactly the same.
   - **Zones** — The number of and names of zones must be exactly the same. Note that zone names are case-sensitive.
     - For any cluster configuration, a minimum of three zones must exist in this configuration domain.
     - The zone creation order must be exactly the same.
     - A dedicated heartbeat zone and interface must be configured on each firewall.
       The heartbeat zones of the HA pair must be directly physically connected with the appropriate cable:
       - 100baseT NIC — Use a crossover cable.
       - 1000baseTX NIC — Use a standard Cat5e or Cat6 cable.
   - For any cluster configuration, a minimum of three zones must exist in this configuration domain.

2) Verify the following requirements for load-sharing clusters:
   - The firewalls must not have IPv6 enabled.
   - The firewalls must have identical hardware configurations.
   - The interface that is used for the heartbeat zone must be at least as fast as the fastest load-sharing interface on your firewall.
   - The switches that are connected to the firewalls must meet certain requirements, depending on the layer 2 mode that you configure for the cluster.
   - [For firewall version 7.0.1 or later] The Unicast - mirrored and the Unicast - flooded layer 2 modes are supported only on *em* and *igb* NICs.
   - [For firewall version 7.0.1 or later] If VLAN interfaces that share the same parent NIC or NIC group are configured to use either the Unicast - mirrored or the 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 (either Unicast - mirror or Unicast - flooded).

   Note: A load-sharing cluster enforces these requirements by maintaining the synchronization of the cluster MAC address and the layer 2 mode of the appropriate VLAN interfaces.

Configure the heartbeat interfaces

You must configure a dedicated heartbeat zone and interface on each firewall *before* configuring an HA cluster.

Note: This procedure is not applicable to firewalls on X-Series Platforms.

You can perform this configuration either in the Control Center Client Application after the firewall has been added to and registered with the Control Center Management Server or you can configure the heartbeat interfaces in the Admin Console.

Note: The heartbeat zone cannot have IPv6 enabled. You must have at least one IPv4 address for each heartbeat interface.

Steps

1) Make sure that each firewall has an interface that can be dedicated to HA traffic.

   Note: Do not use a VLAN for the heartbeat zone.

2) For this procedure, the firewalls must have already been added to the Control Center and their objects must have been retrieved successfully.

3) In the Control Center Client application, create a heartbeat zone.
   a) In the navigation bar, select **Policy**.
   b) Click the **Rule Objects** tab.
   c) Expand the **Network Objects** node.
   d) Expand the **Zones** node.
   e) Double-click the **Zones** node. The **Zones** window is displayed.
   f) Specify **heartbeat** in the **Name** field. The **Description** field is optional.
   g) In the **Firewall** column, select the name of the firewall that you are defining this heartbeat zone for.
   h) Select the **Respond to ICMP echo and timestamp** check box.

      Note: Do not select **Hide port unreachables** for a heartbeat zone.

   i) Click **OK** and save your changes.

4) Configure the heartbeat zone for an interface on the firewall.
   a) In the **Policy** tree, expand the **Firewalls** node.
   b) Double-click the firewall that you are defining the interface for. The **Firewall** window is displayed.
   c) In the tree on the left, select **Interfaces**. The **Firewall Interfaces** tab is displayed in the **Interfaces** area by default.

d) Edit the heartbeat zone for an existing interface or create a new interface that includes the heartbeat zone.

- To edit an existing interface, enter the IP address in the IP address column and select **heartbeat** as the value of the Zone column. Select a NIC for this interface if there is not one selected already. Edit other fields as needed.
- To create a new interface that includes the heartbeat zone, click **+**. A new row is added to the list of interfaces. To configure this interface, click **Advanced** in that row. The **Firewall Interface** window is displayed. Make sure that **heartbeat** is selected as the value of the **Zone** field. Select a NIC in the **NIC or NIC group** list and make other edits as needed.

e) Click **OK** in the **Firewall** window to save your changes.

5) Repeat 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.

Result

Now you can create a cluster from these two firewalls.

Create a cluster in Control Center

You can create a one-node or a two-node cluster from a registered firewall by using the **Cluster Wizard**.

Before you begin

Make sure that your firewalls have conformed to all of the following prerequisites:

- Cluster requirements are met
- Heartbeat interfaces are configured

Both procedures begin with selecting one firewall from the list of registered firewalls. As you work through the wizard, you will specify the second firewall for the two-node cluster.

Note: This procedure is not available for firewall clusters on X-Series Platforms.

To create a one-node or two-node cluster:

Steps

1) Navigate to the **Cluster Wizard**.

a) In the navigation bar, select **Policy**.

b) In the **Policy** tree, expand the **Firewalls** node.

c) Right-click the firewall that you will use for the two-node cluster or the one-node cluster and select **Create/Join Cluster**. The **Cluster Wizard** is displayed.

2) On the **Welcome to the Cluster Setup Wizard** page, if you have met all the prerequisites, click **Next**. The **Cluster State** page is displayed.

3) Depending on what you want to do, select **Create 1-node cluster** or select **Create cluster with 2 nodes** and click **Next**. The **Create Cluster** page is displayed.

4) Specify a name for the cluster. For two-node clusters, also select the firewall that is going to be the second cluster member in the **Choose the second node** field.

   Then click **Next**. The **High Availability (HA) Mode** page is displayed.

5) Configure the high availability feature.

   a) Select the mode for this cluster and click **Next**.

      - If you select **Primary/Standby HA** as the mode, the **High Availability (HA) Layer 2 Mode** page is displayed. Skip to Step c.
      - If you selected either of the other two mode options, the **Takeover Time** page is displayed.

   b) On the **Takeover Time** page, specify the takeover time and click **Next**.

      - If you selected **Load-Sharing** as the mode, the **High Availability (HA) Layer 2 Mode** page is displayed.
      - If you are configuring any other mode, the **High Availability (HA) Shared Cluster Addresses** page is displayed. Skip to Step d.

   c) On the **High Availability (HA) Layer 2 Mode** page, select the default L2 mode for this cluster and click **Next**. The **High Availability (HA) Shared Cluster Addresses** page is displayed.

   d) On the **High Availability (HA) Shared Cluster Addresses** page, configure the shared cluster IP address for at least three interfaces and select the heartbeat zone that contains the heartbeat interface. Then click **Next**.

      - If the IP management address of the cluster can be determined, the **High Availability (HA) Advanced General Properties** page is displayed. Skip to Step f.
      - If the IP management address of the cluster *cannot* be automatically determined, the **Cluster Management Address** page is displayed. This can occur when the selected firewall is behind NAT.

   e) On the **Cluster Management Address** page, specify the cluster management address. Note the IP address or addresses that are displayed in the **Cluster Member Management Address** field if you need to create a new NAT rule for this cluster. Then click **Next**. The **High Availability (HA) Advanced General Properties** page is displayed.

   f) On the **High Availability (HA) Advanced General Properties** page, specify the values for **IPSec authentication** and **High Availability identification** and click **Next**. The **Cluster Wizard Summary** page is displayed.

6) On the **Cluster Wizard Summary** page, if the information is correct, click **Finish**. The **Apply Configuration** window is displayed with the cluster node selected in the list of firewalls.

7) In the **Apply Configuration** window, the new cluster node is selected in the list of firewalls. You must apply the configuration for the process to be completed. Configure the settings to schedule the apply or click **OK** to perform it now. The **Configuration Status** page is displayed after the apply process starts so that you can track the progress.

   Note: After the node configuration is applied, the new cluster node is restarted, except for firewall version 7.0.1.01 or later, where only some of the services will be restarted.

8) After the apply configuration is completed, verify that the cluster was created by expanding the **Clusters** node and then the **Firewalls** node. You should see the new cluster node under the **Clusters** node and the firewall (one-node cluster) or firewalls (two-node cluster) should no longer be listed under the **Firewalls** node.

Create a cluster on the Forcepoint Sidewinder Admin Console

You can create a cluster on the Forcepoint Sidewinder Admin Console and not on the Control Center Client.

After you create the cluster on the Admin Console, you must move to the **Policy** icon of the Control Center Client application. The following procedures define this process at a high level.

Note: This procedure is not available for clusters on X-Series Platforms.

Steps

1) From the Forcepoint Sidewinder Admin Console, perform the following steps.
   a) Define the High Availability (HA) configuration and the cluster nodes and cluster interfaces.
   b) Register the firewall cluster that is to be managed by the Control Center.

2) From the Control Center Client application, perform the following steps.
   a) In the navigation bar, select **Policy**.
   b) In the **Policy** tree, add a new cluster object by right-clicking the **Clusters** node and selecting **Add Object**. The **Add New Cluster Wizard** is displayed.

      Tip: For option descriptions, press **F1**.

   c) Proceed through the **Add New Cluster Wizard**. Make sure to also register the cluster as part of this wizard. After you have completed the **Add New Cluster Wizard**, the cluster node objects are created and their names are displayed beneath the cluster object node in the **Policy** tree.
   d) Apply the changes to the cluster.
   e) Double-click the cluster object to display the **Cluster** window.

      All the common objects that are handled by the HA cluster are represented in the window. The **High Availability** area has the common parameters of the cluster object. Make configuration changes as needed.

f) Double-click one of the cluster member node objects to display the **Cluster Member** window.

   Configuration parameters that are specific to the cluster member node are represented in this window. The **High Availability** area has the HA settings that are *unique* to the selected cluster member node. Make configuration changes as needed.

Add and register pre-existing clusters

You can add and register a pre-existing cluster to the Control Center by using the **Add New Cluster Wizard**.

Before you begin

The following prerequisites must have already been configured:

- The Control Center must be able to have SSH access to the firewall.
- If this cluster is any other Forcepoint Sidewinder appliance for version 8.0.0 or earlier, you must configure this SSH access on the firewall. Use the Admin Console to enable the SSH access control rule on this firewall for external sources and destinations. After you save this change, you can go to the Control Center Client application and run the **Add New Cluster Wizard**.

Note: If the cluster for X-Series Platform has already been created on that appliance, this access is already been configured on the firewall.

To define or create a cluster from firewalls that are already registered and added to the Control Center, use the **Cluster Wizard**.

To add and register the cluster:

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, double-click the **Clusters** node. The **Add New Cluster Wizard** is displayed.

   Tip: For option descriptions, press **F1**.

3) Complete the information on the **Firewall Connection Information** page and click **Next**. The **Firewall Registration Information** page is displayed.

4) Register the firewall with the Control Center Management Server.

   Note: To skip the registration process, on the **Firewall Registration Information** page, click **Next**. The **Retrieval of the firewall into Control Center** page is displayed. Skip to Step 5.

   a) On the **Firewall Registration Information** page, select the **Register the firewall with this Management Server** checkbox.

   b) Click **Next**. The **Summary** page is displayed.

c) On the **Summary** page, verify the information that you have configured. If it is correct, click **Register**; if not, correct any problems. The **Registration Status** page is displayed.

d) On the **Registration Status** page, view the progress of the firewall registration. After it successfully completes, click **Next**.

5) To retrieve items and categories from the firewall into Control Center, on the **Retrieval of the Firewall into Control Center** page, select the items and categories to be retrieved and click **Finish**. These objects are retrieved and the cluster is displayed in the list of clusters in the **Policy** tree.

> **Note:** The icon that represents the firewall cluster on X-Series Platform in the **Clusters** tree is different from the one that is used for Forcepoint Sidewinder cluster. (The cluster member node icons are the same for both types of clusters.)

Managing clusters

The Control Center allows you to manage firewall HA clusters and particular nodes that are in the cluster. This management accommodates monitoring functions.

Join an existing cluster

You can configure a standalone firewall to join an existing cluster in the **Cluster Wizard**.

> **Note:** This procedure is not available for firewall clusters on X-Series Platforms.

The following restrictions apply for the firewall that you are promoting in this procedure:

- The cluster already has two member nodes.
- The cluster that you selected does not have any member nodes.
- The version number of the existing cluster member does not match the version of the firewall that you are about to promote.

To join a firewall to an existing cluster:

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Firewalls** node.

3) Right-click the firewall node that will be joining the cluster and select **Create/Join Cluster**. The **Cluster Wizard** is displayed.

> **Tip:** For option descriptions, press **F1**.

4) On the **Welcome to the Cluster Setup Wizard** page, click **Next**. The **Cluster State** page is displayed.

5) Select **Join existing cluster** and click **Next**. The **Join Cluster** page is displayed.

6) On the **Join Cluster** page, select the cluster object to join. The **FQDN** of the existing cluster member is displayed. Click **Next**. The **Cluster Wizard Summary** page is displayed.

7) On the **Cluster Wizard Summary** page, if the information is correct, click **Finish**. The **Apply Configuration** window is displayed with the cluster node selected in the list of firewalls.

8) In the **Apply Configuration** window, the cluster node is selected in the list of firewalls. You must apply the configuration for the process to be completed. Configure the settings to schedule the apply or click **OK** to perform it now. The **Configuration Status** page is displayed after the apply process starts so that you can track the progress of it.

Note: After the node configuration is applied, the firewall (cluster node) is restarted, except for firewall version 7.0.1.01 or later, where only some of the services will be restarted. The original primary node will also be restarted in the same manner as the new node.

9) After the apply configuration is completed, verify that the join actually occurred by expanding the targeted cluster node and then the **Firewalls** node. You should see the new cluster member under the cluster node and it should no longer be listed under the **Firewalls** node.

Modify configuration data for a cluster

You can add or change configuration information for a cluster in the **Cluster** window.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Clusters** node.

3) Double-click the cluster node to edit. The **Cluster** window is displayed.

4) Configure the fields on this window as needed.

Tip: For option descriptions, press **F1**.

5) Click **OK** to save your changes.

Modify cluster interface properties

You can modify interface configuration information on the cluster in the **Cluster Interface Properties** window.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Clusters** node.

3) Double-click a cluster in the tree. The **Cluster** window for the selected node is displayed.

4) In the tree on the left, expand the **Interfaces** node. The **Cluster Interfaces** area is displayed.

5) Double click any interface row. The **Interface Properties** window is displayed.

6) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

7) Click **OK** to save your changes.

Cluster member demotion

You can demote one or both cluster members from a cluster by using the **Cluster Wizard**. When you demote both cluster members to standalone firewalls at the same time, the cluster is also deleted.

Note: For firewall clusters on X-Series Platforms, you cannot demote cluster members. You can only delete cluster members.

The following procedures are available for cluster member demotion:

- **Demote one cluster member (node) to a standalone firewall** — When a single cluster member of a multi-member cluster is demoted for a firewall cluster that is not on X-Series Platform, the following actions take place:
  - Any object that is referenced by the cluster will be copied to the new standalone firewall, except for the objects listed below.
  - The following objects are excluded because they will remain with the cluster and will not be associated with the new standalone firewall:
    - Interface aliases
    - VPN peers with cluster or alias gateway addresses
    - VPN bypasses
- **Demote all the cluster members to standalone firewalls** — [Not available for firewall clusters on X-Series Platforms] When all the cluster members in a cluster are demoted (whether that is one cluster member in a single-node cluster or both members of a two-node cluster), all the objects from the cluster are copied to the standalone firewalls.

Demote one cluster member (node) to a standalone firewall

You can use the **Cluster Wizard** to demote one cluster member.

Before you begin

Before you access the **Cluster Wizard** to perform a demotion, the objects in the cluster must have been retrieved at least once—that is, its member and interface information must already exist in the Control Center Management Server database.

This proceedure applies to the following senarios:

- The cluster member is a member of a two-cluster member cluster
- The cluster member is the only member of a cluster

Note: This procedure is not available for a firewall cluster on X-Series Platform.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Clusters** node.

3) Expand the cluster node that contains the cluster member to be demoted.

4) Right-click the cluster member and select **Demote to Standalone**. The **Cluster Wizard** window is displayed.

5) If all the objects for the cluster have been retrieved at least once in Control Center, on the **Welcome to the Cluster Setup Wizard** page, click **Next**. The **Cluster Wizard Summary** page is displayed.

6) On the **Cluster Wizard Summary** page, all changes that have been made in this wizard are displayed. Click **Finish** to demote the cluster member in this cluster. The selected cluster member is now moved to the list of firewalls in the **Policy** tree and the **Apply Configuration** window is displayed.

7) In the **Apply Configuration** window, both the cluster node and the demoted cluster member are selected in the list of firewalls. You must apply configurations to both of these objects for the demotion to be completed. Configure the settings to schedule the apply or click **OK** to perform it now. The **Configuration Status** page is displayed after the apply process starts so that you can track the progress.

8) After the configurations are applied, verify that the demotion actually occurred.

   Before you access the **Cluster Wizard** to perform a demotion, the objects in the cluster must have been retrieved at least once—that is, its member and interface information must already exist in the Control Center Management Server database.

   If there were two cluster member nodes in this cluster and you just demoted one, you should still see the other cluster member node in the cluster, and the demoted member should now appear as a standalone firewall under the **Firewalls** node.

   If there was only one member node in the cluster and you just demoted it, the member node should now be displayed as a standalone firewall under the **Firewalls** node, and the cluster node should be deleted from under the **Clusters** node.

Related concepts

Cluster member demotion on page 288

Demote all the cluster members to standalone firewalls

You can demote all the cluster members in a cluster to standalone firewalls by using the Cluster Wizard. This procedure also deletes the cluster node.

Before you begin

Before you access the **Cluster Wizard** to perform this type of a demotion, the cluster must have been retrieved at least once—that is, its member and interface information must already exist in the Control Center Management Server database.

Note: This procedure is not available for clusters on X-Series Platforms.

Steps

1) In the navigation bar, select **Policy** and expand the **Clusters** node.

2) Right-click the cluster node and select **Demote Cluster**. The next interface that is displayed depends on whether there are configured interface aliases in this cluster.
   - If there are configured interface aliases, the **Cluster Wizard** window is displayed. Go to the next step.
   - If there are no configured interface aliases, the **Cluster Wizard Summary** page is displayed. Skip to Step 7.

3) In the **Welcome to the Cluster Setup Wizard** page, click **Next**.

   If the following conditions are met, the **Resolve Interface Aliases** page is displayed:
   - The entire cluster is being demoted—that is, the cluster node and its member nodes.
   - There is more than one cluster member in this cluster node.
   - The cluster node has at least one configured interface alias.

4) On the **Resolve Interface Aliases** page, in the **Associate these addresses with the selected firewall** field, specify the firewall that will be demoted and that will accept the alias address associations. The alias IP addresses and subnet masks that are associated with this firewall are also displayed.

5) [Conditional; 8.1.x and later firewalls] You are presented with the option to delete shared addresses, or to retain them. If you choose to retain them, select the node the addresses are assigned to.

6) Click **Next**.

   - If the following conditions are met, the **Resolve VPN Objects** page is displayed:
     - The entire cluster is being demoted—that is, the cluster node and its member nodes.
     - There is more than one cluster member in this cluster node.
     - The cluster node has at least one configured VPN object that cannot be automatically resolved. This includes VPN peer objects that have a cluster (non-alias) gateway address and VPN bypass objects.
   - If there are no configured VPN objects that must be manually resolved, the **Cluster Wizard Summary** page is displayed. Skip to Step 9.

7) On the **Resolve VPN Objects** page, in the **Associate these VPN objects with the selected firewall** field, specify the cluster member (firewall) that will be demoted and that will accept the VPN object associations. The type, name, gateway IP address, and description information for the selected VPN object are also displayed.

   Click **Next**. The **Cluster Wizard Summary** page is displayed.

8) On the **Cluster Wizard Summary** page, all changes that have been made in this wizard are displayed. Click **Finish** to demote all the cluster members in this cluster. Note that the rules set of the cluster will be associated with each firewall. The **Apply Configuration** window is displayed.

9) In the **Apply Configuration** window, both of the demoted cluster member are selected in the list of firewalls. You must apply configurations to both of these objects for the demotion to be completed. Configure the settings to schedule the apply or click **OK** to perform it now. The **Configuration Status** page is displayed after the apply process starts so that you can track the progress.

10) After the configurations are applied, verify that the demotion actually occurred.

    Expand the **Clusters** node to see that the cluster node is no longer there. Then expand the **Firewalls** node to verify that both firewalls are listed there.

Related concepts

Cluster member demotion on page 288

Delete a cluster member on X-Series Platforms

You cannot demote cluster member nodes from firewall clusters on X-Series Platforms within the Control Center Client application. However, you can delete them.

The reverse is true for firewall clusters that are not on X-Series Platforms. You can demote them, but not delete them.

Note: You also cannot delete the primary cluster member node of a cluster on X-Series Platform.

If, at some later time, you decide to add this cluster member node back into the firewall cluster on X-Series Platform, you must do that directly on the appliance.

Steps

1) In the navigation bar, select **Policy**.

2) Expand the **Clusters** node.

3) Expand the cluster node that contains the cluster member that you want to delete.

4) Right-click the cluster member to be deleted, and select **Remove Object(s)** or press **Delete**. A confirmation message is displayed.

5) Click **Yes** to continue.

   The **Delete Firewall** window is displayed only if there are dependent objects that are associated with this object.

6) Configure the fields on the **Delete Firewall** window as needed.

   Tip: For option descriptions, press **F1**.

7) Click **Delete Firewall** to delete the cluster member node. A confirmation message is displayed.

8) Click **OK**. An informational message is displayed about the need to apply these changes.

9) If you click **Yes**, the change is applied and the cluster member node is deleted. If you click **No**, the cluster member is temporarily deleted until the next time that data is retrieved from the cluster, which is a short interval of time.

View cluster information on X-Series Platforms

For clusters on X-Series Platforms only, you can view information that is not available to you in the **Cluster** window in the user interface of the cluster from within the Control Center Client application.

To view this system and operational data for the cluster on X-Series Platform, make sure that you have specified the IP address or URL of this cluster in the **Hostname/IP address** field in the **Appliance Address** area of the **General** area on the **Cluster** window.

You can now view system and component operational information about the cluster X-Series Platform on the **Launch UI** page. You cannot perform any configurations here.

Note: To perform configurations, you must access the cluster on X-Series Platform directly by using an SSH client. Use the Secure Shell window to access the cluster on X-Series Platform by using an SSH client.

To access the native user interface of the cluster node, use the right-click menu:

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, expand the **Clusters** node.

3) Right-click the node of the cluster on X-Series Platform that you want to access and select **Launch UI**. A security alert message is displayed.

4) Click **Yes** to proceed. The logon page is displayed within the Client work area.

5) Specify your user name and password and click **Login**. The **Launch UI** page is displayed.

   For additional help while you are within the application, click **?** or see the documentation that was included with the application.

6) When you have finished, click **Sign out** to exit this application.

Configure device groups

A *device group* is a collection of one or more firewalls or clusters that can be managed as a group. Create groups of related device objects that will be managed as one entity in the **Device Group** window.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, double-click the **Device Groups** node. The **Device Group** window is displayed.

3) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

4) Click **OK** to save your changes.

CHAPTER 21

Rules

Contents

Rules provide the mechanism for applying policy for your firewalls. They determine the way that the firewall processes network traffic.

How rules are used to process connections

Rules determine how the firewall processes connections through or to the firewall.

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

- **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

Rule elements

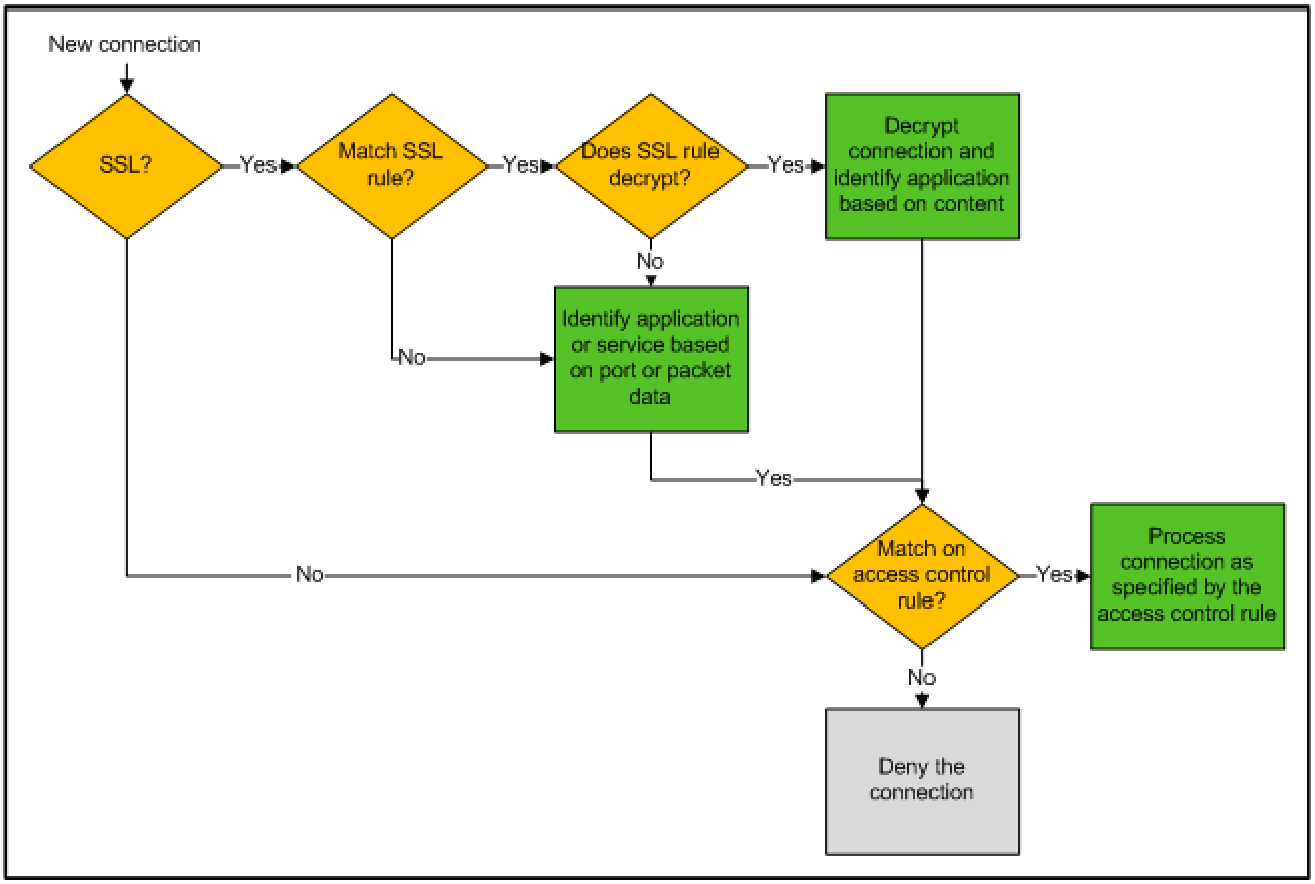
Rules are defined by two types of elements.

- **Conditions** — Determine whether a connection matches a rule
- **Action** — Specifies the ways that the firewall processes a connection

When the firewall processes a new connection, it consults access control rules and SSL rules to determine how to proceed.

This process is displayed in the following figure.

Figure 18: Rule processing


New connection
SSL?
Yes
Match SSL rule?
Yes
Does SSL rule decrypt?
Yes
Decrypt connection and identify application based on content
No
Identify application or service based on port or packet data
No
Yes
No
Match on access control rule?
Yes
Process connection as specified by the access control rule
No
Deny the connection

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

- 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.
- If an SSL connection is decrypted by an SSL rule, the content of the connection is examined to identify the application.

The access control rule that matches the SSL connection must take into account whether the connection was decrypted by an SSL rule because 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 26: Rules to allow HTTPS connections

Decrypted by SSL rule?	Application identified as...	Application required on the access control rule
Yes	HTTP	The following options are available: • **SSL/TLS** — Matches all the applications inside of the SSL connection • **HTTP** — Matches only HTTP-based applications inside of the SSL connection • **HTTP-based application** — Matches only this specific application inside of the SSL connection (for example, Facebook)
No	SSL/TLS	SSL/TLS

How access control rules work

Access control rules provide the network security mechanism that controls the flow of data into and out of the internal network.

When a packet arrives, the firewall scans the access control rules list from top to bottom looking for a rule match. The first access control rule that matches the defined packet criteria is applied. All subsequent access control rules are ignored. If no access control rule matches, the packet is denied. Any traffic that is not specifically allowed is prohibited.

Access control rules specify the network communications protocols that can be used to transfer packets, the hosts and networks where packets can travel to and from, and the time periods when the access control rules can be applied. Access control rules are created by the system administrator and should reflect the security policy of the internal network site.

Types of access control rules

There are two different types of access control rules.

- **Allow rules** — These permit a connection to proceed to its destination after the firewall inspects it.
- **Deny and drop rules** — These prevent a connection from reaching its destination. A deny rule notifies the sender that the request was rejected, whereas a drop rule does not perform this notification. Note that a connection is also denied if it does not match any of the active allow rules.

Access control rules are session-level rules. A network session is a traffic stream between two endpoints. It consists of many datagrams and is identified by a signature that includes the following components:

- Source address
- Destination address
- Protocol
- Source port
- Destination port

The packet filter maintains a record of all the sessions that it has seen and maintains the state that is associated with a session.

Importance of rule order

The display order of the access control rules and nested groups in your security policy is significant.

When the firewall receives a packet, it searches the enabled access control rules in sequential order (beginning with the first rule or nested group within the group, then the second, and so on). If the traffic does not match the first access control rule, it is forwarded to the next rule. The first access control rule that matches all the characteristics of the connection request (service, source, destination, and so on) manages the connection. After an access control rule match is found, the traffic is processed according to that rule and the search stops.

Guidelines for defining your security policy with access control rules

These guidelines will help you organize and maintain your security policy.

- Organize access control rules based on the frequency they are used. If you expect an access control rule to be widely used, such as a rule granting company-wide outbound HTTP access, place that rule near the beginning of your policy.
- Place specific access control rules before general rules. If you want to deny access to one group, such as contractors, while still allowing access for employees, place the access control rule that is denying contractors' access *before* the rule that is allowing employees' access.
- Audit your access control rules periodically. Look for rules that are no longer in use and rules that can be combined by using groups, such as service groups, netgroups, or Application Defense groups.

The default policy contains a Deny All access control rule at the end of the policy. This rule denies any traffic that reaches it. The access control rule is a reminder that any traffic that does not match a rule is automatically denied. Even if the access control rule is deleted, the firewall denies any traffic that does not find an exact match in your security policy.

Access control rule interactions

The Control Center Client application allows you to view all the access control rules that interact with the access control rule that you are currently editing.

Analysis is performed on the **Interactions** tab of the **Access Control Rule Editor** window. Every access control rule that is displayed on this tab does, in some way, interact with the baseline rule (that is, the access control rule that you have selected to edit in this window).

The analysis is based on the value or values in every field. The system determines whether the values of a field are the same, whether one is a superset of the other, whether one is a subset of the other, or whether they intersect (that is, share one or more common values). Also considered in the analysis is the priority or position of each rule. (Remember that access control rules are run in top-down order.)

Rule interactions are available only on enabled access control rules.

How access control rules interact

Use the **Interactions** tab to view rule interactions.

Access control rules can intersect in many different ways. Some of these intersections might be intentional. However, sometimes this intersection can cause unintended results that can be difficult to troubleshoot.

The **Interactions** tab on the **Access Control Rule Editor** window provides a visual way to view the intersections. The rule that you are editing in the **Access Control Rule Editor** window is displayed in **bold**. This will be referred to in this section as the baseline rule. The other rules that are displayed either above or below the baseline rules all intersect with the baseline rule in some way. These will be referred to as intersection rules in this section. Again, every intersection rule on this tab intersects with the baseline rule in one of the following ways:

- **Completely obscuring or completely obscured** — Intersecting rules that precede the baseline rule might *completely obscure* the baseline rule when the values of all the fields in the intersecting rule are equal to or a superset of the values of the corresponding fields of the baseline rule.

  Similarly, intersecting rules that follow the baseline rule might be *completely obscured* by the baseline rule when all the fields in the intersecting rule are equal to or a subset of the values of the corresponding fields of the baseline rule. This type of interaction is not expected in a list of rules. When an intersecting rule completely obscures or is completely obscured by the baseline rule, an error icon is displayed at the beginning of the row and the fields that are the probable cause of this condition are shaded in red. Intersecting rules that are exactly the same as the baseline rule are also in this category and are easily noticed because all the fields in the row are shaded in red.
- **Partially obscuring or partially obscured** — Intersecting rules that precede the baseline rule might *partiallyobscure* the baseline rule when one or more fields of the intersecting rule are a subset of the values of the corresponding field or fields of the baseline rule, and other fields are equal.

  Similarly, intersecting rules that follow the baseline rule can be *partially obscured* by the baseline rule when one or more fields of the intersecting rule are a superset of the values of the corresponding field or fields of the baseline rule, and other fields are equal.

  This type of interaction is expected in a list of rules; the more specific rules should be positioned toward the top of the list and the more general rules should be positioned later.

  On the Interactions tab, these partially obscuring or partially obscured intersecting rules have already been identified because they are displayed in the table. However, these fields and rules have no unique icons or shading. You can learn more about these intersections at the field level by viewing the ToolTip for each field.
- **Complex** — When the values of some of the fields of an intersecting rule are supersets of the values of corresponding fields in the baseline rule, values of some of the other fields are subsets, and other fields are equal, the rules have a *complex* relationship. Although some traffic might match either rule, the rules partially obscure each other, regardless of the order that the rules are placed in. This condition is not expected in a list of rules.

  Rules can also have a complex relationship with each other if any field of an intersecting rule has some values that are included in the corresponding field of the baseline rule and some values that are not the same, and the corresponding field of the baseline rule also has some of the same values as those in the intersecting rule and some that are not the same. If any field of an intersecting rule has a complex relationship with the baseline rule and all other fields of each rule intersect in some way, the relationship of the intersecting rule to the baseline rule is complex. For example, if the baseline rule matches the internal zone and the dmz zone, and another rule matches the dmz zone and the external zone, neither zone value is a subset of the other. The dmz zone value exists in each rule and the other values (internal zone and external zone) are unique. When an intersecting rule has a complex relationship with the baseline rule, the intersecting rule is displayed with a warning icon and the complex fields or completely obscuring fields are shaded in green.

Intersecting access control rules example

This example illustrates two different outbound access control rules, where a preceding rule has an intersection of port values and source values.

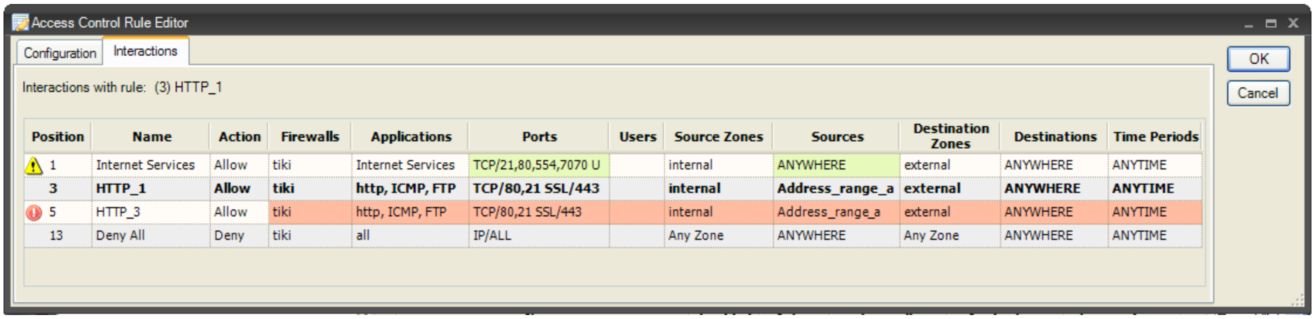
In the following table, note the common (shared) ports and the unique ports. Because each rule has unique ports that the other rule does not have, the preceding intersecting rule is classified as a complex rule.

Table 27: Example of a complex rule intersection

Rule Name	Position	Ports	Shared Ports	Unique Ports
Internet Services	1	TCP/21,80,554,7070 UDP/554	TCP/21,80	TCP/554,7070 UDP/554
HTTP_1	**3**	**TCP/80,21 SSL/443**		**SSL/443**

In the following figure, the complex rule that was discussed above is displayed. Additionally, there is a completely obscured rule (HTTP_3) that has exactly the same field values as the baseline rule (HTTP_1). Note the visual indicators for these two types of intersections. Also, note that other intersecting fields do not have shading or icons. However, they do display ToolTips that indicate the nature of the interaction with the baseline rule value.

Figure 19: Example of complex, completely obscured, and expected rule intersection



Interactions with rule: (3) HTTP_1

Position	Name	Action	Firewalls	Applications	Ports	Users	Source Zones	Sources	Destination Zones	Destinations	Time Periods
⚠ 1	Internet Services	Allow	tiki	Internet Services	TCP/21,80,554,7070 U		internal	ANYWHERE	external	ANYWHERE	ANYTIME
3	**HTTP_1**	**Allow**	**tiki**	**http, ICMP, FTP**	**TCP/80,21 SSL/443**		**internal**	**Address_range_a**	**external**	**ANYWHERE**	**ANYTIME**
❗ 5	HTTP_3	Allow	tiki	http, ICMP, FTP	TCP/80,21 SSL/443		internal	Address_range_a	external	ANYWHERE	ANYTIME
13	Deny All	Deny	tiki	all	IP/ALL		Any Zone	ANYWHERE	Any Zone	ANYWHERE	ANYTIME

Interactions tab ToolTips and access control rule details

In addition to shading and icons, ToolTips and rule details also provide information about the fields on the **Interactions** tab.

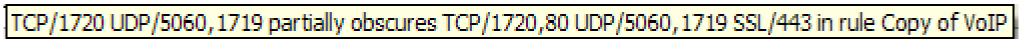
Interactions tab ToolTips

Every field in the **Interactions** tab has a ToolTip that explains the interaction between the value in the intersecting rule with the value of the baseline rule.

Tip: Most of these fields do not have table cell shading. Therefore, you might want to hover over other fields to view interaction details.

The following example occurs in an intersecting rule (**VoIP**) that intersects with the baseline rule (**Copy of VoIP**). The **VoIP** rule is not flagged with an icon or shading. However, if you hover over the value in the **Ports** field of the **VoIP** rule, the information in the following figure is displayed in the ToolTip.

Figure 20: Example of ToolTip



TCP/1720 UDP/5060,1719 partially obscures TCP/1720,80 UDP/5060,1719 SSL/443 in rule Copy of VoIP

As you can see, the ToolTip indicates that the value in the intersecting rule (**VoIP**) partially obscures the value in the baseline rule (**Copy of VoIP**). It also provides the intersect information. The **Copy of VoIP** rule has one additional port (SSL/443) as compared to the **Internet Services** rule.

Interactions tab access control rule details

You can view the details about any rule that is displayed on the **Interactions** tab by double-clicking it.

The details of the rule are displayed, in read-only mode, in the **Access Control Rule Details** window.

Access control rule management

Use the **Access Control Rules** page and various other related windows to view and prioritize your access control rules.

View access control rules

View all currently configured access control rules.

Steps

1) In the navigation bar, select **Policy**.

2) Do one of the following.
   - View access control rules for all firewalls. If you have a combination of firewall version 7.x and 8.0.0 or later appliances that are registered to the Control Center, click the **Access Control Rules** tab.
     - Click **7.x Firewall Rules (Service-Based)** tab to view 7.x rules. The page for that 7.x rules appears in the work area.
     - Click **8.x Firewall Rules (Application-Based)** tab to view 8.x rules. The page for 8.x rules appears in the work area.
   - View access control rules for a specific firewall:.

   a) Expand the **Firewalls** node in the **Policy** tree.

   b) Right-click the firewall node that you want to see rules for and select **View Rules**.
   The **Access Control Rules** page appears for the selected firewall.

   > **Tip:** For option descriptions, press F1.

Navigational options on the Access Control Rules page

Several options are available when you are working with access control rules and rule groups on the **Access Control Rules** page.

- Moving access control rules and access control rule groups
  - Drag the access control rule or rule group to the new position. You can drag a single access control rule to another position or you can drag the access control rule into a rule group.

  - Use the tools on the **Access Control Rules** page to move a selected access control rule or rule group up or down one position or to the top or to the bottom of the **Access Control Rules** page.
  - [Access control rules only] Click **Move to Position**. The **Move to Position** window appears.
- Filtering the access control rule display
  Use the **Filter** and **Find** fields on the **Access Control Rules** page to retrieve only those access control rules that meet certain filter constraints.
- Adding objects to access control rules from the **Rule Objects** tree
  Drag certain objects from the **Rule Objects** tree on the left to the column of the same name for a specific access control rule on the **Access Control Rules** page. The following objects can be dragged: firewalls, services (for version 7.x firewalls) or applications (for version 8.0.0 firewalls or later), sources, destinations, time periods, and zones (to either the **Source Zones** or **Destination Zones** column).

  Note: You cannot drag a zone object if **Any Zone** or **All Zones** are selected.

  If a zone object is dragged to a column that already has a zone object, the new zone is added to the list of zones. If a zone object is dragged to a column that contains one or more zone group objects, or a zone group object is dragged to a column that contains zone objects, the zone object is not added to the list of zones.
- Replacing objects in access control rules
  Use the **Search and Replace** window to search for and replace the following types of objects in your access control rules: network objects, service objects, and firewalls.
- Viewing data about some of the objects directly on the **Access Control Rules** page
  Use the mouse to hover over the following column data on the **Access Control Rules** page to view more information:
  - **IP address information** — View IP address information for a value in the **Sources** or **Destinations** column.
  - **Port information for services** — View port information for a value in the **Services** column (for firewall version 7.x).
  - **Protocol and port information for applications** — View protocol and port information for a value in the **Applications** column (for firewall version 8.0.0 or later).
- Exporting access control rule data
  Use the **Export Access Control Rules** window to configure settings to export the data in all your access control rules to an external file.
- Changing the display of the group hierarchy in your access control rules
  You can expand or collapse all the groups or only the currently selected group of access control rules in the tree by selecting one of the following right-click options: **Expand Selected Group and Subgroups**, **Expand All Groups**, or **Collapse All Groups**.
- Changing the row height of a particular row in the table
  Move the mouse to the first column in the table of the row to be edited. When the cursor changes shape, you can drag the top or bottom of the row to a new height.
- Removing access control rules from one or more firewalls
  Use the **Firewalls in Access Control Rules** window to add or remove selected access control rules from one or more firewalls.

Move a rule to a specific position

Move a rule to a different position.

You can move a rule to a new position or insert an existing rule into a rule group by dragging it to the targeted position. For individual rules (but not rule groups), you can use this window to move the rule to a new position.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab or **Other Rules** > **SSL Rules**. The **Access Control Rules** page or the **SSL Rules** page appears in the work area.

3) Select the rule to move and click the **Move To Position** tool. The **Move to Position** window appears.

   Tip: For option descriptions, press **F1**.

4) Type the new position in the **Move to position** field, or use the up and down arrows to select the new position.

5) Click **OK**.

Result

The rule appears in the new position. The other rules move up or down to accommodate the moved rule.

Customize the Access Control Rules page view

Select the columns that are displayed on the **Access Control Rules** page.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page appears in the work area.

3) In the toolbar, click **Access Control Rule Columns**. The **Access Control Rule Columns** window appears.

   Tip: For option descriptions, press **F1**.

4) Use the left and right arrows to move columns between the **Visible Columns** and **Available Columns** lists.

5) Use the up and down arrows to arrange columns in the **Visible Columns** list as desired.

6) Click **OK**.

Result

The columns listed in the **Visible Columns** list appear on the **Access Control Rules** page in the order selected.

Create access control rule groups

Organize sequences of access control rules into rule groups that can be saved and managed as objects.

You can create access control rule groups that do not contain any access control rules or a single rule. You can also specify an access control rule group that contains one or more nested rule groups.

Steps

1) In the navigation bar, select **Policy**.
2) Click the **Access ControlRules** tab. The **Access Control Rules** page appears in the work area.
3) [Optional] You can select an access control rule to add to a group or you can wait until after you have created the group.
4) Right-click the selected access control rule or right-click anywhere in the work area and select **Add Group**. The **Rule Group** window appears.

   Tip: For option descriptions, press **F1**.
5) Enter a name and description for the rule group.
6) Click **OK**.

Result

The new group is added to the **Access Control Rules** list.

Add or edit an access control rule

Create a new access control rule or to modify an existing one.

Steps

1) In the navigation bar, select **Policy**.
2) Navigate to the **Access Control Rules** page. Do one of the following:
   - Right-click a specific firewall or cluster in the Policy tree and select **View Rules**.
     The **Access Control Rules** page appears.
   - [Conditional] If the Control Center manages only version 7.x firewalls or only version 8.0.0 or later firewalls, click the **Access Control Rules** tab.
     The **Access Control Rules** page appears.
   - [Conditional] If the Control Center manages both version 7.x firewalls and version 8.0.0 or later firewalls, click the **Access Control Rules** tab, then click the **7.x Rules (Service-Based)** tab or the **8.x Rules (Application-Based)** tab as appropriate.
     The **Access Control Rules** page appears for the respective version.

3) Open the **Access Control Rule Editor** window.

- If you are creating a new rule, click **Add**.
- If you are editing an existing rule, select the rule, then click **Edit**.

The **Access Control Rule Editor** window appears.

Tip: For option descriptions, press **F1**.

4) Configure the fields on this window as needed.

When you select your endpoints (sources and destinations), there are some guidelines that you must follow regarding IPv4 and IPv6 endpoints, depending on the support that the selected applications provide:

- If all the selected applications support IPv6 endpoints, you can configure IPv6 endpoints in the Sources, Destinations, NAT, and Redirect fields. All these fields must have the same address family—either all IPv6 or all IPv4 addresses.
- If all the selected applications support IPv4 address translation, IPv6 endpoints can be used in the Sources, Destinations, NAT, and Redirect fields. All these fields must have the same address family, except for the Sources field, which can contain an IPv4 address when all selected applications support IPv4 address translation.
- Only HTTP applications support IPv4 address translation.

5) Click **OK**.

Result

New access control rules are added to the **Access Control Rules** page. Changes to existing rules are saved.

Use identities in access control rules

Browse identities (users and groups from the firewall, external authentication servers, or Active Directory servers) if you are configuring users and user groups for an access control rule.

Note: You must have communication with a McAfee Logon Collector (MLC) server configured to browse MLC users, groups, and distribution lists.

Steps

1) Navigate to the **Identity Browser** window.

2) In the navigation bar, select **Policy**.

3) Display the **Access Control Rules** page.

a) If you have a combination of version 7.x and 8.0.0 or later firewalls that are registered to the Control Center, click the **Access Control Rules** tab. Then click the **8.x Rules (Application-Based)** tab. The **Access Control Rules** page appears in the work area.

b) If you have only version 8.0.0 or later firewalls that are registered to the Control Center, click the **Access Control Rules** tab. The **Access Control Rules** page appears in the work area.

4) In the toolbar, click **Add** to add a new rule or click **Edit** to edit an existing rule. The **Access Control Rule Editor** window appears.

5) In the Users and user groups list, click **Advanced Search**.

   a) If you have MLC server communication configured, the **Identity Browser** window appears.

   b) If you do not have MLC server communication configured, a warning appears. Click **OK**. The **Identity Browser** window appears.

   Tip: For option descriptions, press **F1**.

6) Select the identities to use in the access control rule.

7) Click **OK**.

Result

The selected identities appear in the **Users and user groups** list in the **Access Control Rule Editor** window.

Use identities in firewall user groups

Browse identities (users and groups from the firewall, external authentication servers, or Active Directory servers) if you are configuring a firewall user group.

Note: You must have communication with a McAfee Logon Collector server configured to browse MLC users, groups, and distribution lists.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Rule Objects** tab.

3) Expand the **Firewall Users** node.

4) Double-click the **User Groups** node for a new user group or double-click an existing user group. The **User Group** window appears.

5) In the **User groups** table, select a user group and click **Find members**.

   a) If you have MLC server communication configured, the **Identity Browser** window appears.

   b) If you do not have MLC server communication configured, a warning appears. Click **OK**. The **Identity Browser** window appears.

   Tip: For option descriptions, press **F1**.

6) Select the identities to use in the firewall user group.

7) Click **OK**.

Result

The selected identities appear in the **User Groups** list in the **User Group** window.

Replace objects in access control rules

Replace or modify network objects, service objects, or firewalls that are used by multiple access control rules.

For example, if you need to change a server that is being used in your access control rules, you can make the changes all at one time, instead of having to edit each access control rule individually.

The following guidelines apply when replacing objects in access control rules:

- **Domain objects** — You can replace domain objects only with domain objects.
  You cannot replace a domain object with a network object of another type (such as a host, network, and so on). To view all the network object types, see the Network Objects tree in the Policy tab.
- **Network protocols** — You cannot replace an IPv4 network object with an IPv6 network object.
  You can replace objects only of the same protocol type. (For example, replace one IPv6 object with another IPv6 object). You can also replace ANY_IPv4 with ANYWHERE because these objects have the same behavior in access control rules.
- **Services** — [For version 7.x firewalls only] You can replace one service with another service only if they both are the same service type and have the same agent. This also means that you cannot replace a single service with a service group.
- **Firewalls** — The following guidelines apply to firewalls:
  - **Versions** — Both firewalls must be the same version. Additionally, if you are working with version 7.0.1 or later firewall objects, they both must have the same IPv6 enabled state. (This state is defined on the Firewall window.)
  - **Replacing a firewall with a device group** — Each firewall in the group must comply with the versions criteria that is mentioned above.
  - **Replacing a device group with a single firewall** — At least *one* firewall in the device group must match the version and IPv6 enabled state of the target single firewall.
  - **Replacing a single firewall with ALL FIREWALLS** — You can perform this replacement only if all the firewalls in this configuration domain are the same version.
  - **Replacing ALL FIREWALLS** — You can replace this object with any firewall, regardless of firewall version or IPv6-enabled states.
  - **Replacing one device group with another device group** — This is not allowed.

Steps

1) Make sure you have the following administrative privileges:
   - Access to the ALL FIREWALLS object (that is displayed in the **Apply On** list in the **Access Control Rule Editor** window)
   - Ability to update access control rules in this configuration domain
   - Ability to update privileged rules

   If you do not have all these privileges, a message appears when you click **OK**.

2) In the navigation bar, select **Policy**.

3) Click the **Access Control Rules** tab. The **Access Control Rules** page appears in the work area.

4) In the toolbar, click **Search and Replace**. Or you can right-click any rule and select **Search and Replace**. The **Search and Replace** window appears.

Tip: For option descriptions, press **F1**.

5) Select the object to be replaced and the object that will replace it.

6) Click **OK**.

Result

The object is replaced in all access control rules.

Convert network objects in access control rules for the IPv6 protocol

Enable IPv6 functionality in a configuration domain.

CAUTION: This is a global, configuration domain-wide change. The conversion cannot be undone.

When IPv6 is enabled, two default network objects are available for access control rules and SSL rules to distinguish between ANYWHERE endpoints:

- ANY_IPv4
- ANY_IPv6

You are given the opportunity to ANYWHERE network objects in existing IPv4 access control rules to ANY_IPv4 network objects. You can also choose *not* to change the ANYWHERE objects.

If you decide not to convert the ANYWHERE objects in this window and change your mind about this later, use the Search and Replace window to replace these objects or other network or service objects.

Steps

1) Make sure you have the following user privileges:
   - Access to all firewalls
   - Ability to update access control rules
   - Ability to update system objects
   - Ability to access privileged objects

2) In the navigation bar, select **Policy**.

3) In the Policy tree, select the **Firewalls** node.

4) Double-click a firewall in the tree. The **Firewall** window for the selected firewall appears.

5) Make sure that the General area appears. Select **Enable IPv6**.
   - If you have the correct user privileges, the **IPv4 Rule Conversion** window appears.

     > **Tip:** For option descriptions, press **F1**.

   - If you do not have the correct privileges, a message appears. Contact your system administrator to obtain these privileges.

6) Select a conversion option.

7) Click **OK**.

Result

IPv6 is enabled for this firewall. If you selected Convert ANYWHERE rules to IPv4, all source or destination endpoints of ANYWHERE in current access control rules are changed to ANY_IPv4.

Associate firewalls with one or more access control rules

Associate firewalls or device groups with one or more selected access control rules.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page appears in the work area.

3) [Conditional] If you have a combination of version 7.x and 8.0.0 or later registered firewalls, click the version-specific tab for those rules to modify.

4) On the **Access Control Rules** page, select one or more access control rules to be modified. To select multiple access control rules, press **Shift** and then click the first and last access control rule to be included in the selection.

5) In the toolbar, click **(Firewalls in Access Control Rules)**. The **Firewalls in Access Control Rules** window appears.

   > **Tip:** For option descriptions, press **F1**.

6) Select the firewalls to add or remove from the selected rules.

7) Click **OK**.

Export access control rule settings to a file

Export your access control rule settings to a text file so that you can have a separate record of the rules that you have configured on the Management Server.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page appears in the work area.

3) In the toolbar on the Access Control Rules page, click **(Export Access Control Rules)**. Or you can right-click any rule and select **Export Access Control Rules**. The **Export Access Control Rules** window appears.

   Tip: For option descriptions, press **F1**.

4) Select the export file format.

5) Select the columns to include and arrange them in the desired order.

6) Click **Export**.

Configure default settings for the access control rule template

Create a template that contains default configuration settings for creating a new access control rule.

Note: By default, new access control rules have the following settings.

Table 28: Default new access control rule settings

Option	Value
Rule Type	Proxy
NAT	Host mode (The **Host** option is selected in the NAT list and **localhost** is selected in the Host list.)
Zones (for Sources)	One must be selected for each access control rule.
Zones (for Destinations)	One must be selected for each access control rule.

You can establish different defaults for all those values making it easier to create access control rules. However, you should also be aware of the following implications of establishing these defaults:

- These settings will be shared among all the users in this configuration domain. You must configure default settings for each configuration domain separately.
- Although you can set the default name prefix in this window, the user is not required to use this prefix when he or she is creating a new access control rule.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page appears in the work area.

3) In the toolbar on the **Access Control Rules** page, click **New Access Control Rule Template**. The **New Access Control Rule Template** window appears.

   Tip: For option descriptions, press **F1**.

4) Define the default values you want to include in the template.

5) Click **OK**.

Result

Whenever you create a new rule, the **Access Control Rule Editor** opens with the default values you selected already populated.

How SSL rules work

Secure Socket Layer (SSL) rules determine whether the firewall decrypts SSL connections. Regardless of an SSL rule match, SSL connections must also match an access control rule to pass through the firewall.

Use an SSL rule in the following scenarios:

- You want to use Application Defenses to inspect SSL connections.
- An SSL application cannot be identified unless the connection to it is decrypted.

For examples of action and type combinations for SSL rules, see the *Forcepoint Sidewinder Product Guide*.

Related concepts

SSL rule management on page 311

SSL rule management

You can perform various management tasks on your SSL rules by using the SSL Rules page and various other related windows.

View SSL rules

You can view your decryption policy as specified in your SSL rules.

Note: This page is available only for firewall versions 8.0.0 or later.

Changes that are made on the SSL Rules page are automatically saved. Changes that are made by using the drag option generate a confirmation message. Use the SSL Rule Editor window to change other settings or to specify the settings for a new rule.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab and select **SSL Rules**. The **SSL Rules** page appears in the work area.

   Tip: For option descriptions, press **F1**.

Navigational options on the SSL Rules page

Several options are available when you are working with SSL rules on the **SSL Rules** page.

- Moving SSL rules
  - Drag the SSL rule to the new position.
  - Use the tools on the **SSL Rules** page to move a selected SSL rule up or down one position or to the top or to the bottom of the **SSL Rules** page.
  - Click **Move to Position**. The **Move to Position** window appears.
- Filtering the SSL rule display
  Use the **Filter** and **Find** fields on the **SSL Rules** page to quickly retrieve only those SSL rules that meet certain filter constraints.
- Changing the row height of a particular row in the table
  Move the mouse to the first column in the table of the row to be edited. When the cursor changes shape, you can drag the top or bottom of the row to a new height.

Add or edit an SSL rule

You can define a new SSL rule or to edit an existing one.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab and then select **SSL Rules**. The **SSL Rules** page appears in the work area.

3) Click **Add** to create a new SSL rule, or select an existing SSL rule and click **Edit**.The **SSL Rule Editor** window appears.

4) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

5) Click **OK** to save the SSL rule.

Override keys and local certificates in SSL rules

You can change the default settings for RSA keys, DSA keys, or local CA certificates.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab and then select **SSL Rules**. The **SSL Rules** page appears in the work area.

3) Click **Add**. The **SSL Rule Editor** window appears.

4) In the **Apply On** field, select at least one firewall.

5) From the **Action** list, select **Decrypt / Re-encrypt** or **Decrypt Only**. The **SSL Decryption Settings (Client to Firewall)** tab is enabled.

6) Click **Override Certificate Settings**. The **Override Certificate Settings** window appears.

   Tip: For option descriptions, press **F1**.

7) Select an override mode and default values for the certificate types for each firewall.

8) Click **OK**.

Configure cipher suites that are allowed in an SSL rule

You can specify the TLS and SSL Cipher Suites to allow or deny for the SSL rule.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab and then select **SSL Rules**. The **SSL Rules** page appears in the work area.

3) Click **Add**. The **SSL Rule Editor** window appears.

4) In the **Apply On** field, select at least one firewall.

5) From the Action list, select **Decrypt / Re-encrypt** or **Decrypt Only**. This **SSL Decryption Settings (Client to Firewall)** tab is enabled.

6) Click **Override Certificate Settings**. The **Override Certificate Settings** window appears.

7) Select an override mode and specify at least one new setting in any of the columns.

8) Click **OK** to save your changes.

9) Click **Allow Selected TLS/SSL Cipher Suites**. The **TLS/SSL Cipher Suites** window appears.

> **Tip:** For option descriptions, press **F1**.

10) Select the cipher suites to allow and click **OK**.

Customize the SSL Rules page view

You can define the columns to display and the order to display them in on the **SSL Rules** page.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab and select **SSL Rules**. The **SSL Rules** page appears in the work area.

3) In the toolbar, click **SSL Rule Columns**. The **SSL Rule Columns** window appears.

> **Tip:** For option descriptions, press **F1**.

4) Use the left and right arrows to move columns between the **Visible Columns** and **Available Columns** lists.

5) Use the up and down arrows to arrange columns in the **Visible Columns** list as desired.

6) Click **OK**.

Result

The columns listed in the Visible Columns list appear on the **SSL Rules** page in the order selected.

How URL rules work

Use URL translation to configure your firewall to redirect inbound HTTP connections by examining application layer data, rather than transport layer data like conventional redirect rules.

By examining the HTTP application layer data, the firewall determines the internal web server where inbound requests are destined—even if multiple servers share the same external IP address.

Use URL translation if your network environment matches one or more of the following scenarios:

- You have multiple websites that resolve by using DNS to a single IP on your firewall.
- You have a one or more websites that contain resources that are hosted on different physical servers behind your firewall.

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. 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 rules to determine the internal web server where the request should be sent.

3) If you select the **Rewrite URL** checkbox, 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 that was determined in Step 2, an access control rule match is performed.

5) If an access control rule is matched, the connection is redirected to the internal web server.

View URL rules

View the URL rules that have been defined on your system.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab.

3) In the list, select **URL Rules**. The **URL Rules** page appears.

   Tip: For option descriptions, press **F1**.

Add or edit a URL rule

Create a new URL rule or to edit an existing one.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab.

3) In the list, select **URL Rules**. The **URL Rules** page appears.

4) Select either **Add New** or **Edit** in the toolbar. The **URL Rule Editor** window appears.

5) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

6) Click **OK** to save this rule.

CHAPTER 22

Policy in action

Contents

The topics in this section contain policy scenarios that use multiple elements of firewall policy.

Conditions for scenarios

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.

Related concepts

How rules are used to process connections on page 295
How access control rules work on page 297
How SSL rules work on page 311

Allow a custom application

Use the Control Center to create a custom application that combines the attributes of an existing application with new ports.

Create a custom application to override the ports of an application in the application database.

Assume that you want to allow MySQL connections on a non-standard port like TCP 11500. To do so, complete the following tasks.

Create a custom MySQL application

Create a custom application that is based on the MySQL application.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Application Objects** node.
4) Double-click **Custom Applications**. The **Custom Application** window is displayed.
5) Configure the custom application.
   a) In the **Name** field, specify **MySQL on port 11500**.
   b) In the **Parent application** area, select **Other**.
   c) In the **Select parent application** field, type **MySQL**, then select the **MySQL** application.
   d) In the **Ports** area, in the **TCP ports** field, specify **11500**.
   e) Click **OK**.
6) Save your changes.

Use the custom application in an access control rule

Create an access control rule that uses the custom application that you have just created.

Steps

1) In the navigation bar, select **Policy**.
2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Allow MySQL on port 11500**.

6) In the **Action** list, select **Allow**.

7) In the **Applications** area, select **MySQL on port 11500**.

8) Configure the **Sources** and **Destinations** areas as appropriate.

9) Click **OK** to save your changes.

Allow inbound access to internal servers

To allow inbound access to internal servers, create inbound redirect access control rules.

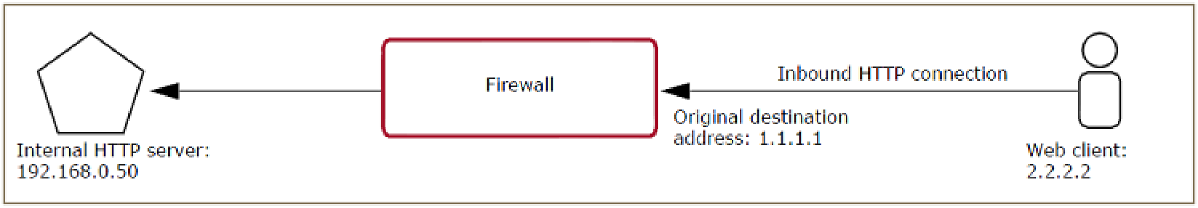
There are two ways to redirect inbound connections:

Redirect based on application

You can configure an inbound redirect rule to forward a connection that is destined for an external firewall IP address to an internal server. Redirection works based on connection elements such as application, source, and destination.

Assume that you want to allow HTTP connections from the Internet to reach an internal HTTP server, as shown by the following figure. The external client (2.2.2.2) initiates a connection to the firewall external IP address (1.1.1.1). The firewall redirects the connection to the appropriate internal server (192.168.0.50).

Figure 21: Redirection in action


Firewall
Inbound HTTP connection
Original destination address: 1.1.1.1
Internal HTTP server: 192.168.0.50
Web client: 2.2.2.2

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

Table 29: 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 that is used in the preceding examples, perform the follwoing tasks.

Create network objects

Create network objects for the internal HTTP server and the firewall external IP address.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Network Objects** node.
4) Double-click **Hosts**. The **Hosts** window is displayed.
5) Create a network object for the internal HTTP server.
    a) In the **Name** field, specify **Internal web server**.
    b) In the **Address** field, specify **192.168.0.50**.
6) Click **OK** to save your changes.
7) Create an additional network object for the firewall external IP address.
    a) Repeat Step 4.
    b) In the **Name** field, specify **Firewall external IP**.
    c) In the **Address** field, specify **1.1.1.1**.
8) Click **OK** to save your changes.

Related tasks
Create an inbound redirect access control rule on page 320

Create an inbound redirect access control rule

Create an access control rule to redirect inbound HTTP connections to your internal HTTP server.

Steps

1) In the navigation bar, select **Policy**.
2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.
3) Select the **8.x Firewall Rules (Application-Based)** tab.
4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify a name for the access control rule, such as **Inbound redirect to HTTP server**.

6) Make the following selections, using the two new network objects that you just created for the **Destinations** and **Redirect values** as indicated:

Option	Selection
Action	**Allow**
Applications	**HTTP**
Source	**Any_IPv4**
[Sources] Zones	**Selected zones** > **external**
Destinations	Firewall external IP
[Destinations] Zone	**Selected zones** > **external**
NAT	**NONE**
Redirect	Internal web server

7) Click **OK** to save this rule.

8) Move the new access control rule above the **Deny All** rule.

Redirect HTTP based on URL

Use URL translation to configure your firewall to redirect inbound HTTP connections based on the URL that is contained in the HTTP request.

By examining the HTTP application layer data, the firewall determines the internal web server where inbound requests are destined, 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 websites that resolve by way of DNS to a single IP address on your firewall.
- You have a website that contains resources that are hosted on different physical servers behind your firewall.

Note: URL translation is not compatible with inbound SSL content inspection.

If URL translation is enabled on an Internet-facing zone, inbound HTTP requests are handled in the following way:

Steps

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 application layer data of the HTTP request and compares it to the defined URL translation rules to determine the internal web server that the request should be sent to.

3) [If **Rewrite URL** is enabled in the URL rule] 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 that was determined in Step 2, an access control rule match is performed.
   - If an access control rule is matched, the connection is redirected to the internal web server.
   - If no access control rules match, the connection is denied.

Create URL rules

Create URL rules to redirect inbound HTTP connections based on application layer data.

Steps

1) In the navigation bar, select **Policy**.

2) From the **Other Rules** tab, select **URL Rules**. The **URL Rules** page is displayed, which contains a list of the configured URL rules.

3) Click **Add** to add a new URL rule. The **URL Rules Editor** window is displayed.

   When you create URL 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; therefore, 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.

4) In the **Name** field, type a descriptive name for this rule.

5) [Optional] In the **Description** field, enter any useful information about this rule.

6) In the **Apply on** list, select the firewall or firewalls that you want this rule to apply to.

7) Configure the fields in the **Source** area.
   a) In the **Zones** field, select the zones or zone groups where the clients that generate the inbound HTTP requests are located.

b) You can select either the **Matching URL** or the **Matching URLattributes** option:

   - When **Matching URL** is selected, 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**, **Port**, and **Path prefix** fields are automatically populated, based on the URL that you enter.
   - When **Matching URL attributes** is selected, complete the **Host**, **Port**, and **Path prefix** fields with the data that is used to match inbound HTTP requests.

8) Configure the fields in the **Destination** area.

   a) In the **Server address** field, select or create an IP address object that corresponds to the internal web server that connections that match this rule should be redirected to.

   b) [Optional] Select **Rewrite URL** 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 **Matching URL** information that you entered in Step 7. Path information beyond the original URL path prefix in the HTTP request is unaffected.

   Select an option:

   - Select **New URL**, then specify 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 are automatically populated, based on the URL that 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 Control Center does not modify hyperlinks in HTML files. Therefore, 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.

9) Click **OK** to save the ULR rule.

Create access control policy to authorize inbound HTTP

URL rules determine only 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 rules.

To create the required access control policy, perform the following tasks.

Create an inbound URL Generic Application Defense profile

Create a Generic Application Defense profile to enable the non-transparent connection type for HTTP.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the Application Defenses node.
4) Double-click the **Generic** node. The window is displayed.
5) Specify a name for the new profile, such as **Inbound URL Generic App Defense**.
6) Click **Connection Settings**. The **Proxy Connection Settings** window is displayed.
7) Enable the non-transparent connection type for HTTP.
   a) Select **Override default connection types**.
   b) In the **Connection Type** field for HTTP, select **Non-Transparent**.
   c) Click **OK**.
8) Click **OK** in the Generic Application Defense window to save your changes.

Create an inbound URL HTTP Application Defense profile

Create an HTTP Application Defense profile to configure enforcement settings for HTTP.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the Application Defenses node.
4) Double-click the **HTTP** node. The **HTTP Application Defense** window is displayed.
5) Define the new profile.
   a) In the **Name** field, specify a name for the new profile, such as **Inbound URL HTTP App Defense**.
   b) In the **Type** field, select **Server**.
6) [Optional] Configure enforcement settings.
   a) On the **General** tab, enable HTTP enforcements as appropriate.

   b) Use the other tabs to configure the enabled enforcements.

7) Click **OK** to save your changes.

Create an inbound URL Application Defense group

Create an Application Defense group that contains the Generic and HTTP Application Defense profiles that you have just created. This Application Defense group will be used by an access control rule.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **Group** node. Double-click on **Default**. The **Application Defense Groups** window is displayed.

5) In the **Name** field, specify a name for the new Application Defense group, such as **Inbound URL group**.

6) In the **Use In** area, select **8.x firewall rules (application-based)**.

7) Select the profiles that you have previously created.

   a) In the **Mapping List** area, go to the **Generic** row and in the **Name** column, select the **Generic Application Defense** profile that you previously created.

   b) In the **HTTP** row, select the HTTP profile that you created.

8) Click **OK** to save your changes.

Create an inbound URL access control rule

Create an access control rule that uses the Application Defense group that you just created.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Inbound URL**.

6) Make the following selections.

Option	Selection
Action	**Allow**
Applications	**HTTP**
[Sources] **Zones**	**Selected zones** > **external**
Destinations	Select all the internal HTTP servers that URL rules redirect connections to
[Destinations] **Zones**	**Selected zones** > **internal** (the zone where the destination servers are located)
Redirect	**NONE**
Application Defense (Group)	**Inbound URL group**

7) [Optional] If you added ports other than 80 to any URL rules, add them to the list of ports.

   a) In the ports field, select **Override ports**.

   b) In the field below this field, specify the additional ports.

8) Click **OK** to save your changes.

9) Move the new access control rule so that it is displayed above the **Deny All** rule.

Allow outbound web access

Use the Control Center to configure the firewall to inspect and control HTTP and HTTPS connections.

These are the protocols that are most often 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

Inspect and control outbound SSL (including HTTPS) on page 358

Allow HTTP and pass-through SSL (including HTTPS)

Assume that you want to inspect outbound HTTP and pass-through SSL (including HTTPS). To do so, create an access control rule that uses the HTTP and SSL/TLS applications.

> **Tip:** 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) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Outbound HTTP and SSL**.

6) Make the following selections.

Option	Selection
Action	**Allow**
Applications	• **HTTP** • **SSL/TLS**
[**Sources**] **Zones**	**Selected zones** > **internal**
[**Destinations**] **Zone**	**Selected zones** > **external**

7) Click **OK** to save the changes.

8) Move the new access control rule above the **Deny All** rule.

Allow HTTP only

Assume that you want to allow HTTP, but not HTTPS or SSL. To do so, create an access control rule to allow HTTP and to override the default ports.

By overriding the ports to remove SSL/443, the rule is prevented from matching HTTPS connections that are decrypted by an SSL rule.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Outbound HTTP only**.

6) Make the following selections.

Option	Selection
Action	**Allow**
Applications	**HTTP**
[Sources] Zones	**Selected zones** > **internal**
[Destinations] Zones	**Selected zones** > **external**

7) To prevent the rule from matching decrypted HTTPS connections on port 443, override the application ports.
   a) In the ports field, select **Override ports**.

   b) In the field below this field, specify **TCP/80**.

8) Click **OK** to save the changes.

9) Move the new access control rule above the **Deny All** rule.

Allow pass-through SSL only

Assume that you want to allow SSL to pass through the firewall without decrypting it. To do so, create an access control rule that uses the SSL/TLS application.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Outbound SSL only**.

6) Make the following selections.

Option	Selection
Action	Allow
Applications	SSL/TLS
[Sources] Zones	Selected zones > internal
[Destination] Zones	Selected zones > external

7) Click **OK** to save the changes.

8) Move the new access control rule above the **Deny All** rule.

Allow IPv6 network flows through the firewall

Use these scenarios as examples when creating IPv6 allow rules for other applications.

Two scenarios are provided: one for an application with native IPv6 support (HTTP), and one for an application that lacks native IPv6 support (SSH).

Note: You must have IPv6 enabled on the firewall for these scenarios.

Related tasks
Enable IPv6 and create IPv6 addresses on a firewall on page 274

Allow HTTP over IPv6

You can make configurations to allow *only* outbound HTTP IPv6 network flows through the firewall. You can use the same approach for other applications that natively support IPv6.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Allow HTTP over IPv6**.

6) Make the following selections:

Note: Key selections are highlighted in bold.

Option	Selection
Action	**Allow**
Applications	**HTTP**
Sources	**Any_IPv6**
[Sources] Zones	**Selected zones** > **internal**
Destinations	**Any_IPv6**
[Destination] Zones	**Selected zones** > **external**

7) Click **OK**.

8) Move the new access control rule above the **Deny All** rule.

Allow SSH over IPv6

You can allow only outbound SSH IPv6 network flows through the firewall. You can use the same approach for other applications that lack native IPv6 support.

Create a custom TCP application

Use this task to create a custom application based on TCP that uses the standard SSH port, port 22.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Objects** node.

4) Double-click **Custom Applications**. The **Custom Application** window is displayed.

5) Configure the custom application.
   a) In the **Name** field, specify **TCP on port 22**.

   b) In the **Parent application** area, select **TCP/UDP**.

   c) In the **Ports** area, in the **TCP ports** field, specify 22.

   d) Click **OK**.

6) Save your changes.

Create an allow rule

Create an IPv6 allow rule that uses the custom application.

Steps

1) Make sure IPv6 is enabled.

2) In the navigation bar, select **Policy**.

3) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

4) Select the **8.x Firewall Rules (Application-Based)** tab.

5) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

6) In the **Name** field, specify **Allow SSH over IPv6**.

7) Make the following selections:

> **Note:** Key selections are highlighted in bold.

Option	Selection
Action	**Allow**
Applications	**TCP on port 22** (custom application)
Sources	**Any_IPv6**
[**Sources**] **Zones**	**Selected zones** > **internal**
Destinations	**Any_IPv6**
[**Destination**] **Zones**	**Selected zones** > **external**

8) Click **OK**.

9) Move the new access control rule above the **Deny All** rule.

Related tasks
Enable IPv6 and create IPv6 addresses on a firewall on page 274

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).

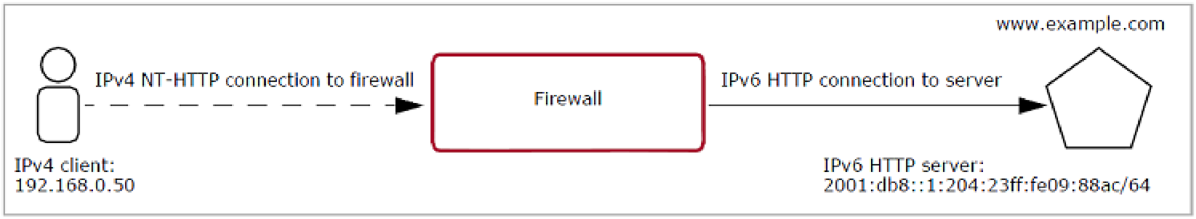
  Tip: The client browsers must be configured to use the firewall IP address as a proxy server.

- 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 an IPv6 address by 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 by using IPv4.

Assume that you want to allow an IPv4 client to reach an IPv6 webserver at www.example.com.

In the following figure, 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 following table shows the required IPv4-to-IPv6 translation rule.

Figure 22: IPv4-to-IPv6 translation


www.example.com
IPv4 NT-HTTP connection to firewall
Firewall
IPv6 HTTP connection to server
IPv4 client:
192.168.0.50
IPv6 HTTP server:
2001:db8::1:204:23ff:fe09:88ac/64

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 30: Example IPv4-to-IPv6 access control rule

[Sources] Zones:**Selected zones** > **internal**	**Destinations zones**: **Selected zones** > **external**
Sources: **192.168.0.50** (internal client)	**Destinations**: **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 an IPv4 to IPv6 Generic Application Defense profile

Create a Generic Application Defense profile to enable the non-transparent connection type for HTTP.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Application Defenses** node.
4) Double-click the **Generic** node. The **Generic Application Defense** window is displayed.
5) In the **Name** field, specify a name for the new profile, such as **HTTP IPv4-to-IPv6**.
6) Click **Connection Settings**. The **Proxy Connection Settings** window is displayed.
7) Enable the non-transparent connection type for HTTP.
   a) Select **Override default connection types**.
   b) In the **Connection Type** field for **HTTP**, 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**
8) Click **OK** in the **Generic Application Defense** window to save your changes.

Create an outbound HTTP Application Defense profile

Create an HTTP Application Defense profile to configure enforcement settings for HTTP.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Application Defenses** node.
4) Double-click the **HTTP** node. The **HTTP Application Defense** window is displayed.

5) Define the new Application Defense.
   a) In the **Name** field, specify a name for the new profile, such as **Outbound HTTP**.

   b) In the **Type** field, select **Client**.

6) [Optional] Configure enforcement settings.
   a) On the **General** tab, enable HTTP enforcements as appropriate.

   b) Use the other tabs to configure the enabled enforcements.

7) Click **OK** to save your changes.

Create an IPv4 to IPv6 Application Defense group

Create an Application Defense group that contains the Generic and HTTP profiles that you previously created. The group will be used by an access control rule.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **Group** node. The **Application Defense Groups** window is displayed.

5) In the **Name** field, specify a name for the new Application Defense group, such as **HTTP IPv4-to-IPv6 group**.

6) In the Use In area, select **8.x firewall rules (application-based)**.

7) Select the profiles that you have previously created.
   a) In the **Mapping List** area, go to the **Generic** row and in the **Name** column, select the Generic Application Defense profile that you previously created.

   b) In the **HTTP** row, select the HTTP profile that you created.

8) Click **OK** to save your changes.

Create an IPv4 to IPv6 access control rule

Create an access control rule that uses the Application Defense group you created.

Steps

1) In the navigation bar, select **Policy**.
2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.
3) Select the **8.x Firewall Rules (Application-Based)** tab.
4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.
5) In the **Name** field, specify **Outbound HTTP IPv4-to-IPv6**.
6) In the **Action** field, select **Allow**.
7) [Optional] To allow non-transparent HTTPS connections on port 80, add SSL/80 to the list of ports.
    a) In the ports field, select **Override ports**.
    b) In the field below this field, specify **TCP/80 SSL/80,443**.
8) Configure the **Sources** and **Destinations** 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_IPv6**.
9) Configure **Advanced** options.
    a) In the **Application defense (Group)** field, select the Application Defense group that you created.
    b) In the **NAT** field, select the firewall external IPv6 address.

    Tip: If the primary external firewall address is IPv6, you can select **localhost**.
10) Click **OK** to save your changes.

Configure non-transparent HTTP

Use the Control Center to configure the firewall to accept non-transparent HTTP connections. In this configuration, the firewall functions as a proxy server.

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 non-transparent HTTP Generic Application Defense profile

Create a Generic Application Defense profile to enable the non-transparent connection type for HTTP.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Application Defenses** node.
4) Double-click the **Generic** node. The **Generic Application Defense** window is displayed.
5) In the **Name** field, specify a name for the new profile, such as **Non-Transparent HTTP**.
6) Click **Connection Settings**. The **Proxy Connection Settings** window is displayed.
7) Enable the non-transparent connection type for HTTP.
   a) Select **Override default connection types**.
   b) In the **Connection Type** field for HTTP, select **Non-Transparent**.

      Tip: If you select **Non-Transparent**, transparent (normal) HTTP connections will not match access control rules that use this profile.

   c) Click **OK**
8) Click **OK** in the **Generic Application Defense** window to save your changes.

Create an outbound URL HTTP Application Defense profile

Create an HTTP Application Defense profile to configure enforcement settings for HTTP.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **HTTP** node. The **HTTP Application Defense** window is displayed.

5) Define the new Application Defense.
   a) In the **Name** field, specify a name for the new profile, such as **Outbound HTTP**.

   b) In the **Type** field, select **Client**.

6) [Optional] Configure enforcement settings.
   a) On the **General** tab, enable HTTP client enforcements as appropriate.

   b) Use the other tabs to configure the enabled enforcements.

7) Click **OK** to save your changes.

Create a non-transparent HTTP Application Defense group

Create an Application Defense group that contains the Generic and HTTP Application Defense profiles that you previously created. The group will be used by an access control rule.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **Group** node. Double-click on **Default**. The **Application Defense Groups** window is displayed.

5) In the **Name** field, specify a name for the new Application Defense group, such as **Non-Transparent HTTP group**.

6) In the **Use In** area, select **8.x firewall rules (application-based)**.

7) Select the profiles that you have previously created.
   a) In the **Mapping List** area, go to the **Generic** row and in the **Name** column, select the Generic Application Defense profile that you previously created.

   b) In the **HTTP** row, select the HTTP profile that you created.

8) Click **OK** to save your changes.

Create an outbound non-transparent HTTP access control rule

Create an access control rule that uses the Application Defense group you created.

Steps

1) In the navigation bar, select **Policy**.
2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.
3) Select the **8.x Firewall Rules (Application-Based)** tab.
4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.
5) In the **Name** field, specify **Outbound Non-Transparent HTTP**.
6) In the **Action** field, select **Allow**.
7) In the **Applications** field, select **HTTP**.
8) [Optional] To allow non-transparent HTTPS connections on port 80, add SSL/80 to the list of ports.
   a) In the ports field, select **Override ports**.
   b) In the field below this field, specify **TCP/80 SSL/80,443**.
9) Configure the **Sources** and **Destinations** areas as appropriate.
10) In the **Application defense (Group)** field, select the Application Defense group that you previously created.
11) Click **OK** to save your changes.

Control access based on user identity

Use Control Center 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 tasks
Configure passive authentication on page 131

Enforce SmartFilter URL filtering for the Sales group

You can configure policy to enforce URL filtering for the Sales group.

To do so, perform the following tasks.

Configure a SmartFilter filter policy

To control the websites that are allowed, denied, and exempt, configure a filter policy.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Firewall Settings** tab.

3) Expand the **SmartFilter** node.

4) Click the **Policies** node. The list of default SmartFilter policies is displayed.
   - If one of default filter policies meets your needs, continue to the next procedure.
     For example, the *Typical_Business_Filter* policy blocks categories that are generally not business-related.
   - To create a custom filter policy, double-click the **Policies** node.

Related tasks
Configure filter policies on page 109

Select the filter policy in an HTTP Application Defense profile

Create an HTTP Application Defense profile that uses the appropriate filter policy.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Double-click the **HTTP** node. The **HTTP Application Defense** window is displayed.

5) Define the new Application Defense.
   a) In the **Name** field, specify a name for the new profile, such as **Sales URL Filtering**.

   b) In the **Type** field, select **Client**.

6) Click the **Content Scanning** tab.

7) Select **Enforce SmartFilter**.

8) Select a SmartFilter policy. In the **Policy** field, select the appropriate filter policy.

9) Click **OK** to save your changes.

Create a URL filtering Application Defense group

Create an Application Defense group that contains the HTTP profile that you previously created.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Application Defenses** node.

4) Expand the **Group** node and double-click **Default**. The **Application Defense Groups** window is displayed.

5) In the **Name** field, specify a name for the new Application Defense group, such as **Sales URL Filtering group**.

6) In the **Use In** area, select **8.x firewall rules (application-based)**.

7) Select the profiles that you have previously created. In the **Mapping List** area, go to the **HTTP** row and in the **Name** column, select **Sales URL Filtering**.

8) Click **OK** to save your changes.

Create a URL filtering access control rule

Create an access control rule that uses the Application Defense group you created.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Sales URL Filtering**.

6) In the **Action** field, select **Allow**.

7) In the **Applications** field, select **HTTP**.

8) In the **Users and user** groups area, select **Sales**.

9) In the **Application defense (Group)** field, select the Application Defense group that you previously created (**Sales URL Filtering group**).

10) Click **OK** to save your changes.

Exempt the Sales manager 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 and does not use SmartFilter.

To create the access control rule:

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Exempt Sales Manager**.

6) In the **Action** field, select **Allow**.

7) In the **Applications** field, select **HTTP**.

8) Add John Smith's identity.

   a) In the Users and user groups area, click **Advanced Search**. The **Identity Browser** window is displayed.

   b) In the **Show** area, make sure that **MLC users** is selected. The list of MLC users is displayed.

   c) Locate John Smith. Select the **Member** checkbox.

   d) Click **OK** to close the Identity Browser window.

9) Click **OK** to save your changes in the access control rule.

10) Move the new rule so that it is above the Sales URL Filtering rule.

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 create the alternative policy:

Steps

1) Create an access control rule group for the alternate policy.

2) In that group, place all the access control rules that are needed to implement that policy.

   Tip: Note that groups can nest within groups.

3) Create a Deny All rule as the last rule of the alternate policy.

4) After the alternate policy is finished, disable it by selecting the main group and deselecting **Enabled**.

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.

Create 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
  - The 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.

Exempt the finance and banking URL category

You can create an SSL rule to prevent connections to finance and banking sites from being decrypted.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab and select **SSL Rules**. The **SSL Rules** page is displayed.

3) In the toolbar, click **Add**. The **SSL Rule Editor** window is displayed.

4) In the **Name** field, specify **Exempt Finance and Banking**.

5) Make the following selections.

Option	Selection
Type	**Outbound**
Action	**No Decryption**
Ports	**<Any>**
Destination (Endpoints)	**Finance/Banking** (URL category)

6) Click **OK** to save your changes.

7) Move the new SSL rule so that it is above the decryption rules that you are exempting connection matches from.

Exempt an application based on port

Assume that you want to exempt an application that uses TCP port 7070 from being decrypted. To do so, create an SSL rule to exempt port 7070.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab and select **SSL Rules**. The **SSL Rules** page is displayed.

3) In the toolbar, click **Add**. The **SSL Rule Editor** window is displayed.

4) In the **Name** field, specify **Exempt Port 7070**.

5) Make the following selections.

Option	Selection
Type	**<Any>**
Action	**No Decryption**
Ports	**7070**

6) Click **OK** to save your changes.

7) Move the new SSL rule so that it is above the decryption rules that you are exempting connection matches from.

Decrypt and inspect SSH content

Use the Control Center to configure the firewall to decrypt SSH connections, perform content inspection, and then re-encrypt the traffic before sending it to its destination.

To decrypt and re-encrypt SSH traffic, the firewall acts in the following ways:

- Like a server when communicating with the client
- Like a client when communicating with the server

The firewall maintains two databases where it stores 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 whether the server host keys that are 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 SSH known host keys database on the firewall.

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 that is 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 to be 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 to be 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 the SSH host key trust level to require to allow the SSH connection to take place. For example:

- Enforce a **Strict** key checking policy for rules that allow access to critical network security devices.
  Host keys with a 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 a **Medium** key checking policy for rules that allow access to non-critical hosts.
  Host keys with a strong or weak trust level are allowed. If a host key is not present in the known hosts database, the client can accept it. When the host key is accepted, it is added to the known hosts database.
- Allow a **Relaxed** key checking policy for rules that are not related to business operations, such as a rule that allows access to an employee's personal computer at home.
  Host keys with a strong or weak trust level are allowed. If a host key is not present in the known hosts database, the client can accept it. When the host key is accepted, it is added to the known hosts database. If a server's host key has changed, the client can accept it. The key then replaces the old key in the known hosts database.

By tailoring key checking policy to the security risk that is involved, you can make sure 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

Use strong host keys when an SSH client connects through the firewall to a device that is critical for the integrity of the network, such as a network security device.

In this scenario, the administrator decides 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 known hosts database of the firewall.

The following configuration steps are necessary to allow the connection to take place:

1) Configure Application Defenses to specify strict key checking policy.
   a) Create an SSH Application Defense profile that enforces a Strict key checking policy.

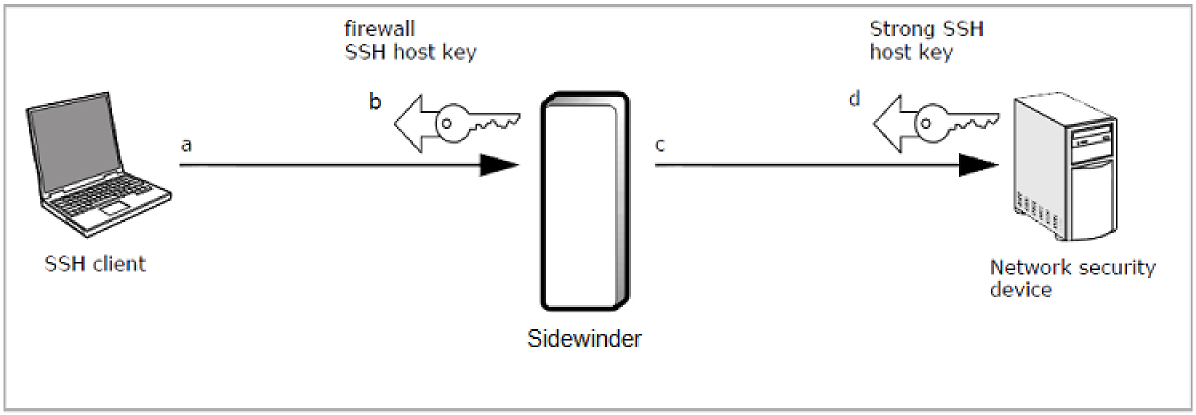
      Note: This requires a strong host key to be present in the SSH known host keys database for the destination SSH server.

   b) Create an Application Defense group that contains the SSH profile that you previously created.

2) Create an access control rule to allow the SSH client to connect to the network security device. The rule must use the following objects:
   - SSH application
   - Application Defense group that you previously created.

3) Import the SSH host key of the network security device into the SSH known host keys database on the firewall and assign a strong trust level to the key.

Figure 23: Example strong SSH known host key scenario



The preceding figure shows the flow when the SSH client initiates an SSH session to the network security device through the SSH proxy agent of the firewall:

a) The client initiates an SSH connection to the network security device. The firewall, acting like an SSH server, accepts the client's connection.

b) The firewall sends its SSH host key to the client.

c) 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.

d) The network security device sends its SSH host key to the firewall.

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

Configure SSH Application Defenses on page 96

Weak host key scenario

Use weak host keys when an SSH client connects through the firewall to a device that is not critical for the integrity of the network, such as an employee connecting to a home computer.

In this scenario, 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 a relaxed key checking policy.

   a) Create an SSH Application Defense profile that enforces a relaxed key checking policy.

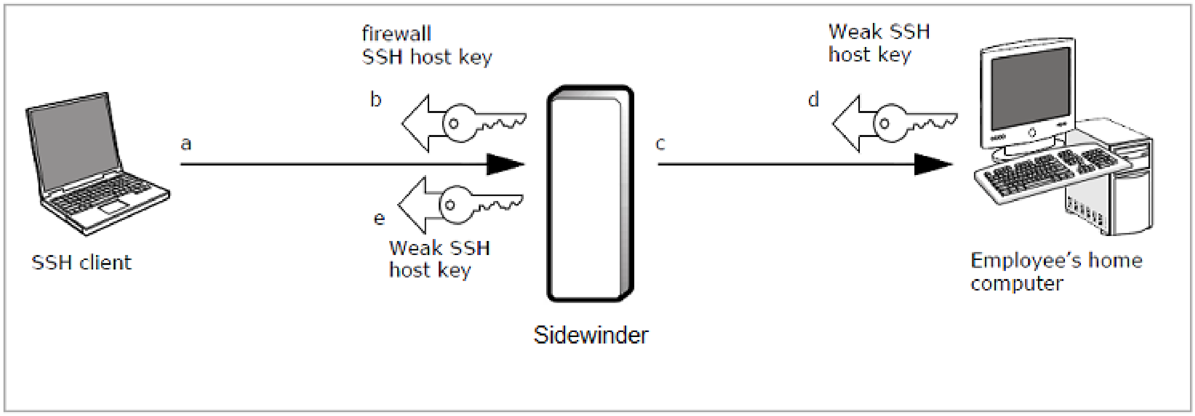
      Note: This allows host keys with a strong or weak trust level. If a host key is not present in the known hosts database, the client can accept it, which adds the host key to the known hosts database. If a server's host key has changed, the client can accept it. The host key replaces the old key in the known hosts database.

   b) Create an Application Defense group that contains the SSH profile that you previously created.

2) Create an access control rule to allow the SSH client to connect to the employee's home computer. The rule must use the following objects:.

   - SSH application.
   - Application Defense group that you previously created.

Figure 24: Example weak SSH known host key scenario



The preceding figure shows the flow when the SSH client initiates an SSH session to the employee's home computer through the SSH proxy agent of the firewall:

a) The client initiates an SSH connection to the employee's home computer. The firewall, acting like an SSH server, accepts the client's connection.

b) The firewall sends its SSH host key to the client

c) 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's connection.

d) The employee's home computer sends its SSH host key to the firewall

e) The firewall sends the SSH host key that is 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 that is presented by the employee's home computer. Because the administrator configured a relaxed key checking policy for the SSH Application Defense, the user has the ability to approve any SSH host key.

Create strong SSH known host keys

Add strong SSH known host keys to enforce strict key checking.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Double-click the **SSH Known Hosts** node. The **SSH Known Hosts** window is displayed.

4) Click **Add Known Host**. The **Add SSH Known Host** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Enter an IP address, port and key type for the new SSH known host.

6) From the **Apply on** drop-down list, select the firewall to apply the known host configuration to.

7) Either retrieve the SSH key from the firewall, or manually enter the SSH key.

8) Click **OK**.

Result

The new SSH server appears on the **SSH Known Hosts** window.

Manage host associations

Delete weak associations from a firewall or promote weak associations to strong associations.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Double-click the **SSH Known Hosts** node. The **SSH Known Hosts** window is displayed.

4) Click **Manage Known Hosts**. The **Manage SSH Known Hosts** window is displayed.

   Tip: For option descriptions, press **F1**.

5) Select the firewall you want to manage host associations for from the drop-down list, then click **Retrieve Weak Associations**. All weak associations for the firewall are listed in the known hosts table.

6) Promote or delete weak associations:

   - To promote a weak association to a strong one, select the **Promote to Strong** checkbox next to the association.
   - To delete a weak association, click **Delete** next to the association.

7) Click **OK**.

Result

Deleted associations are removed from the firewall. Promoted associations appear on the **SSH Known Hosts** window.

Deny access based on country of origin

Use Geo-Location network objects in access control rules to match country of origin.

For this example, assume that your organization needs to prevent users in Country XYZ from accessing a download server to comply with export controls.

To deny all inbound connections from Country XYZ, perform the following tasks.

Create a Geo-Location network object

Create a Geo-Location network object that contains Country XYZ.

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **Network Objects** node.

4) Double-click the **Geo-Location** node. The **Geo-Location** window is displayed.

5) In the **Name** field, specify **Country XYZ**.

6) In the **Available members** list, double-click **Country XYZ**.

7) Click **OK** to save your changes.

Create a deny access control rule

Create an access control rule to deny inbound connections from Country XYZ.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

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

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Deny Country XYZ**.

6) Make the following selections.

Option	Selection
Action	**Deny**
Applications	**all (IP/255)**
[Sources] **Zones**	**Selected zones** > **external**
Sources (Endpoints)	**Country XYZ**
[Destinations] **Zones**	**Selected zones** > **external**

7) Click **OK** to save your changes.

8) Move the new access control rule so that it is above all inbound redirect rules.

Deny access to an application category

Use the Control Center to configure the firewall 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.

Note: Exemption rules must be placed before deny rules.

Assume that you want to configure the following behavior:

- 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.

To achieve this behavior, three access control rules are required.

Table 31: Required access control rules

Rule Position	Application	Action	Users and User Groups
n	**facebook**	**Allow**	Marketing group
n+1	**<Social Networking>**	**Deny**	None specified (matches all users)
n+2	**HTTP**	**Allow**	None specified (matches all users)

Make sure the following prerequisites have been met.

- Passive identity validation is configured on your firewall.
- You have an access control rule in place to allow outbound HTTP.

To deny access to all applications that belong to an application category, perform the following tasks.

Related tasks

Access control rule management on page 301

Configure passive authentication on page 131

Deny access to social networking applications

Create an access control rule to deny access to social networking applications.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Deny Social Networking**.

6) In the **Action** field, select **Deny**.

7) In the **Applications** list, select **<Social Networking>**.

Tip: To find the application category filters more quickly, search for **<**.

8) Click **OK** to save your changes.

9) Move the new access control rule so that it matches the following position requirements:

- It is above your general allow HTTP rule.
- It is below any rules that allow specific social networking applications.

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) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Allow Facebook for Marketing**.

6) In the **Action** field, select **Allow**.

7) In the **Applications** list, select **facebook**.

8) In the **Users and user groups** area, select the **Marketing** group.

9) Click **OK** to save your changes.

10) Move the new access control rule so that it is above the above the Deny Social Networking rule.

Discover the applications that are in use in a zone

Use the Control Center to identify the applications that 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 that is allowed by the rule is identified. The application information is audited for further analysis in the Control Center or syslog servers.

The types of applications that are allowed from the zone determine the types of applications that can be identified.

Table 32: 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
all	All applications

To identify applications that are in use in a zone, perform the following tasks.

Enable discovery for the source zone

Enable application discovery for the internal zone.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Rule Objects** tab.
3) Expand the **Network Objects** node.
4) Double-click the **Zones** node. The **Zones** window is displayed.
5) Select the firewall.
6) Select the **Application discovery** checkbox.
7) Click **OK** to save your changes.

Create a discovery zone 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:

Steps

- Identify applications that are already flowing through your access control rules.
- Create access control rules that are intentionally permissive to allow many applications and to identify them.

Viewing application discovery data

You can view the applications that are in use in the following tools.

- Dashboard
- Applications
- Firewall audit

Related concepts
About application objects on page 71
How the Dashboard is organized on page 381
Managing firewall audit data on page 402

Examine your policy by using the Firewall Policy report

You can display a report that contains comprehensive details about your Control Center policy.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Reports** tab.

3) Select **Policy Report**. The **Policy Report** window is displayed.

   Tip: For option definitions, press **F1**.

4) Select a device, then click **Request Report**.

Result

The report appears on the **Policy Report** page.

Related concepts
Firewall policy reports on page 413

Inspect and control inbound HTTPS

To inspect and control HTTPS and other SSL-encapsulated applications, the firewall must decrypt SSL connections.

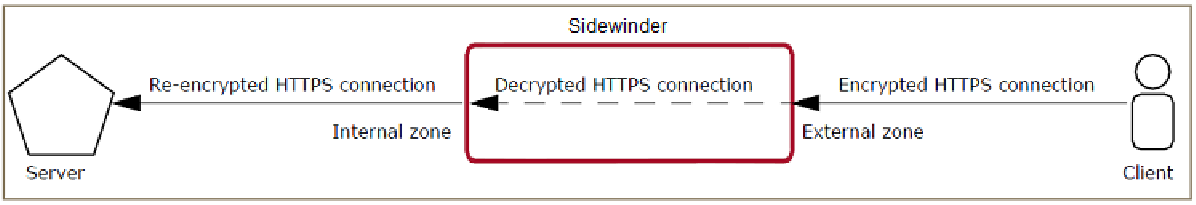
Assume that you want to inspect HTTPS connections from the Internet before allowing them to reach an internal webserver. To inspect inbound HTTPS, you can create two types of inbound SSL rules:

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

Figure 25: Inbound decrypt/re-encrypt connection


Sidewinder
Re-encrypted HTTPS connection
Decrypted HTTPS connection
Encrypted HTTPS connection
Internal zone
External zone
Server
Client

To configure this scenario, perform the following tasks.

Configure inbound HTTPS content inspection

Create a configuration to decrypt, inspect, and re-encrypt inbound HTTPS content.

Configure 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 CA that is trusted by Internet clients.

To configure a CA-signed firewall certificate, work with the CA of your choice.

Related concepts
Certificate management on page 166

Related tasks

Import a firewall certificate on page 168

Load (retrieve) a firewall certificate on page 169

Create an inbound SSL rule

Create an SSL rule to decrypt and re-encrypt inbound SSL connections.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab and select **SSL Rules**. The **SSL Rules** page is displayed.

3) In the toolbar, click **Add**. The **SSL Rule Editor** window is displayed.

4) In the **Name** field, specify **Inspect Inbound SSL**.

5) Make the following selections.

Option	Selection
Type	**Inbound**
Action	**Decrypt/re-encrypt**
Ports	**443**
[Source] Zones	**Selected zones > external**
[Destination] Zones	**Selected zones > external**

6) On the **SSL Decryption Settings (Client to Firewall)** tab, select the CA-signed firewall certificate that you configured. Click the **Override Certificate Settings** button. The **Override Certificate Settings** window is displayed.

   - If the certificate uses RSA keys, select it in the **RSA** list and then select **<None>** in the **DSA** list.
   - If the certificate uses DSA keys, select it from the **DSA** list and then select **<None>** in the **RSA** list.
   - If you configured RSA and DSA certificates, you can select them both.

7) Click **OK** in the **Override Certificate Settings** window to save the changes.

8) Click **OK** to save the changes in the **SSL Rule Editor** window.

9) Move the new SSL rule so that it is above the **Exempt All** rule.

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*>).

Inspect HTTP/HTTPS and deny other SSL

You can create an inbound redirect access control rule for the HTTP application that allows inspected inbound HTTP and HTTPS connections but denies other inbound applications that are using SSL on port 443.

To achieve this behavior, 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.

To create the access control rule:

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Inbound HTTP and HTTPS**.

6) Make the following selections.

Option	Selection
Action	**Allow**
Applications	**HTTP**
[Sources] **Zones**	**Selected zones** > **external**
Destinations (Endpoints)	**Firewall**
[Destinations] **Zones**	**Selected zones** > **external**
NAT	**NONE**
Redirect	**Tip:** Make sure to configure the Web server under **Rule Objects** > **Network Objects** > **Hosts**. Internal web server **Note:** By default, the Redirect port selected is zero. Change this to the port on which the Web server is listening.

7) Click **OK** to save your changes.

8) Move the new access control rule above the **Deny All** rule.

Allow inbound decrypted HTTPS only

Assume that your internal server accepts only HTTPS connections. Therefore, the access control rule should match only HTTPS connections and exclude HTTP connections.

To create the access control rule:

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Inbound HTTPS only**.

6) Make the following selections.

Option	Selection
Action	**Allow**
Applications	**HTTP**
[Sources] **Zones**	**Selected zones** > **internal**
Destinations (Endpoints)	**Firewall**
[Destinations] **Zones**	**Selected zones** > **external**
NAT	**NONE**
Redirect	**Tip:** Make sure to configure the Web server under **Rule Objects** > **Network Objects** > **Hosts**. (Internal web server) **Note:** By default, the Redirect port selected is zero. Change this to the port on which the Web server is listening.

7) To prevent the rule from allowing HTTP connections on port 80, override the application ports.

   a) In the ports field, select **Override ports**.

   b) In the field below this field, delete any values that are there and specify **SSL/443**.

8) Click **OK** to save your changes.

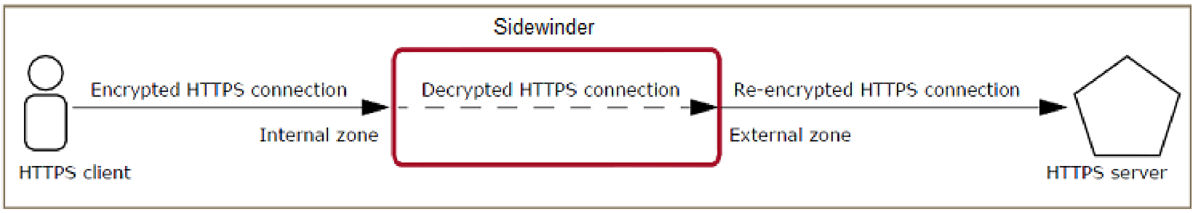
9) Move the new access control rule above the **Deny All** rule.

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.

Assume that you want to inspect SSL connections from internal clients to the Internet. In the following figure, an internal client connects to an external server. The firewall decrypts the connection, inspects it, re-encrypts it, and then forwards the encrypted connection to the server.

Figure 26: Outbound decrypt/re-encrypt connection


Sidewinder
Encrypted HTTPS connection
Internal zone
Decrypted HTTPS connection
Re-encrypted HTTPS connection
External zone
HTTPS client
HTTPS server

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.

To do so, perform the following tasks.

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.

To export the certificate for the firewall CA:

Steps

1) In the navigation bar, select **Policy**.

2) In the lower left area of the window, click the **Rule Objects** tab.

3) Expand the **VPN** node.

4) Click the **CA Certificates** node. The list of CA certificates is displayed.

5) Right-click the **Default_CC_CA** node and select **Export CA Certificate**. The **Export Certificate Wizard** is displayed.

6) Step through the wizard and specify the location where you are exporting this certificate.

7) When you have finished, click **Finish**.

8) 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) In the navigation bar, select **Policy**.

2) Click the **Other Rules** tab and select **SSL Rules**. The **SSL Rules** page is displayed.

3) In the toolbar, click **Add**. The **SSL Rule Editor** window is displayed.

4) In the **Name** field, specify **Decrypt Outbound SSL on 443**.

5) Make the following selections.

Option	Selection
Type	**Outbound**
Action	**Decrypt/re-encrypt**
Ports	**443**
[**Source**] **Zones**	**Selected zones** > **internal**
[**Destination**] **Zones**	**Selected zones** > **external**

6) Click **OK** to save your changes.

7) Move the new SSL rule so that it is above the **Exempt All** rule.

Create access control rules to control 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*>).

Inspect HTTP/HTTPS and deny other SSL on port 443

Create a rule to allow inspected outbound HTTP and HTTPS connections, and deny other applications that are using SSL.

Table 33: Required access control rules

Rule Position	Application	Action	Source zone	Destination zone
n	**HTTP** (matches HTTP and decrypted HTTPS)	**Allow**	**internal**	**external**
n+1	**SSL/TLS** (Matches SSL)	**Deny**	**internal**	**external**

To create the required access control rules:

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) Create a rule to allow outbound HTTP.

6) Create a rule to deny outbound SSL/TLS.

7) Arrange the new rules so that the allow HTTP rule is positioned before the deny SSL/TLS rule.

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) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Outbound HTTPS only**.

6) Make the following selections.

Option	Selection
Action	Allow
Applications	HTTP
[Sources] Zones	Selected zones > internal > Selected zones > internal
[Destinations] Zones	Selected zones > external

7) To prevent the rule from allowing HTTP connections on port 80, override the application ports.
   a) In the ports field, select **Override ports**.

   b) In the field below this field, delete any values that are there and specify **SSL/443**.

8) Click **OK** to save your changes.

9) Move the new access control rule above the **Deny All** rule.

Deny Facebook over SSL

Create a deny access control rule to deny access to Facebook over SSL.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Access Control Rules** tab. The **Access Control Rules** page is displayed.

3) Select the **8.x Firewall Rules (Application-Based)** tab.

4) In the toolbar, click **Add**. The **Access Control Rule Editor** window is displayed.

5) In the **Name** field, specify **Deny Facebook SSL**.

6) Make the following selections.

Option	Selection
Action	**Deny**
Applications	**facebook**
[Sources] **Zones**	**Selected zones** > **internal**
[Destinations] **Zones**	**Selected zones** > **external**

7) [Optional] If you do not want to block access to Facebook over HTTP, override the application ports to remove TCP/80.

   a) In the ports field, select **Override ports**.

   b) In the field below this field, delete any values that are there and specify **SSL/443**.

8) Click **OK** to save your changes.

9) Move the new access control rule above the **Deny All** rule.

CHAPTER 23

Alert processing rules

Contents

When you are managing multiple firewalls, similar alerts that are generated from different firewalls can be difficult to distinguish. Use alert processing rules to evaluate every firewall alert that is being sent to the Management Server to determine the way that the alert will be reported in the **Dashboards** > **Status** page. Additionally, several different types of Management Server alerts are also captured and displayed.

About alert processing rules

Similar to other processing rules, the alerts that are being sent to the Management Server from the firewalls are evaluated by the alert processing rules from top to bottom. The first processing rule that matches the characteristic and condition requirements for the incoming alert is reported in the way in which it has been defined by the rule.

To make sure that all alerts are reported, the last processing rule in the list of rules is generic enough to catch and report any alerts that are not characterized by any of the preceding processing rules.

The Control Center icon provides several different ways for you to manage predefined alert processing rules:

- **View a list of rules** — The table on the **Alert Processing Rules** page displays all the alert processing rules that are currently defined.
- **Edit a rule** — Each processing rule defines alert actions, such as triggering an email message, to associate with the alert. Use the **Alert Processing Rule** window to edit the predefined alert processing rules.
- **Assign a priority level to a rule** — You can assign a priority to a predefined alert processing rule in the **Priority Mapping** window.

View alert processing rules

You can view all the alert processing rules that are available.

Steps

1) In the navigation bar, select **Control Center**.

2) Click the **Alert Processing Rules** tab. The **Alert Processing Rules** page is displayed.

   Tip: For option definitions, press **F1**.

3) Select Management Server or firewall rules.

Result

Alert rules are listed.

Modify predefined alert processing rules

You can edit predefined alert processing rules.

Alert processing rules manage the way in which alerts that are sent from the managed firewalls or from the Management Server are reported.

Steps

1) In the navigation bar, select **Control Center**.

2) Click the **Alert Processing Rules** tab. The **Alert Processing Rules** page is displayed.

3) Do one of the following:

   - Double-click a specific rule.
   - Select the rule to modify, then click **Edit Rule**.

   The **Alert Processing Rule** window is displayed.

   Note: For option definitions, press **F1**.

4) Select the actions that will take place when the alert is triggered.

5) Click **OK**.

Result

The selected actions appear in the **Alert Actions** column for the alert rule.

Assign priority levels to alerts

You can set the priority levels of alerts. You can change the priority of any predefined alert.

These priority maps are shared across all configuration domains. Therefore, if you are modifying the settings of a priority mapping in one domain, that change will proliferate to all the other domains.

Steps

1) In the navigation bar, select **Control Center**.

2) Click the **Alert Processing Rules** tab. The **Alert Processing Rules** page is displayed.

3) In the toolbar, click **Priority Mappings**. The **Priority Mappings** window is displayed.

   Tip: For option definitions, press **F1**.

4) Select the alert processing rule to modify.

5) Select a new priority for the rule.

6) Click **OK**.

CHAPTER 24

Policy validation and application

Contents

When applying a configuration, Control Center sends configuration information to the selected target firewalls.

Control Center transforms and implements the data on the firewall, restarting firewall components as necessary, and reports the results of the task.

Before you apply changes to a firewall, you can validate those proposed changes. The configuration validation process transfers all the related access control rules and configuration data from the Control Center database to the selected firewalls. The receiving firewalls attempt to validate the configuration, but they do not actually apply any changes.

Validate firewall configurations

Make sure firewall configurations stored on the Management Server are valid. You can validate the current firewall configuration or view the differences between the current configuration and the proposed configuration of a firewall.

Steps

1) In the navigation bar, click **Validate**. The **Validate Configuration** window appears.

   Tip: For option descriptions, press **F1**.

2) Select the firewall or firewalls to validate policy on, then click **OK**.

   If there are any issues with the validation, the **Validation Warnings** window is displayed. Do one of the following:

   - Proceed with the validation process, ignoring reported issues The result of this selection is that some of the values that you have configured may not be applicable to the firewall. As a result, the firewall may behave differently than your configuration would suggest.
   - Cancel the validation process This window closes. You can then fix the identified issues and re-validate.

     Note: This action cancels the validation for all selected firewalls, including those firewalls that had no potential issues.

   - Identify a particular type of issue as one that you do not want to see warnings for in the future

   The validation process proceeds. The next time that a validation process is started and a scenario occurs (in which a warning would be displayed), no warning will be issued.

Result

If there are no validation issues, the results of the validation process are displayed on the **Validation Status** page.

Apply firewall configurations

Apply firewall configurations that reside in the Control Center Management Server database.

Any changes that have been made for the firewall in the Control Center Client application will be applied back to the firewall appliance.

You can perform this application immediately or you can schedule it for a later time. When a configuration is scheduled, the current configuration that is stored in the Management Server when the schedule is defined is preserved, along with the status of the checkbox that is used to determine whether the target firewall(s) should be re-initialized.

Configurations can be applied only to firewalls that are currently in communication with the Management Server. Verify the firewall status before applying your changes.

Steps

1) In the navigation bar, click **Apply**. The **Apply Configuration** window appears.

2) [Optional] Select the **Schedule Apply Configuration** checkbox to define a future date and time to apply the configuration. A special date/time window is displayed, in which you can select a date and time when the current configuration is to be applied.

   Note: When you are scheduling a configuration to be applied at a future date and time, the current configuration is preserved and applied at the scheduled time, regardless of configuration changes that have occurred between the time that the apply was scheduled and when the apply occurs.

   When managing an HA pair, only the served firewall will receive configuration information during the configuration propagation. The standby system's configuration is automatically synchronized when the served firewall's configuration has changed.

3) Select the firewall or firewalls to apply the configuration to, then click **OK**.

Result

If there are errors in the apply configuration, the **Apply Warnings** window appears. Do one of the following:

- Proceed with the apply process, ignoring these issues.
  The result of this selection is that some of the values that you have configured may not be applicable to the firewall. As a result, the firewall may behave differently than your configuration would suggest.

  If the apply fails, the **Pending Status** value for this firewall is **! - Apply Failed** on the **Configuration Status** page. You must double-click this firewall on this page to view the errors.

  If the error occurred on a firewall, the message includes a **View Firewall Audit** button, which displays the Forcepoint Sidewinder Audit report. You can view more information about the error that was generated during the apply process.

  If the error occurred on the Control Center Management Server, the message includes a **Details** button, which displays information that you should include when you contact technical support. In this message window version, you can view more information about the error that was generated when the configuration bundle was being created. When you click the **Details** button to display additional information, a **Copy Details** button is also displayed, which copies the information to the Clipboard.

- Cancel the apply process.
  This window closes. You can then fix the identified issues and reapply.

  Note: This action cancels the apply for all your selected firewalls, including for those firewalls that had no potential issues.

- Proceed with the apply process and do not show any warnings in the future.
  The apply configuration process will proceed. When you select this checkbox, the next time that an apply process is started and a scenario occurs (in which a warning would be displayed), no warning will be issued.

If there are no errors, the Control Center sends configuration information to the selected firewalls, transforming and implementing the data on the firewall, restarting firewall components as necessary, and reporting the results of the task back to the Control Center.

The configuration status and any problems that occur while connecting to the firewalls are reported on the **Configuration Status** page. When this page is displayed, the propagation status is refreshed every 15 seconds.

View validation status

Before applying changes to one or more firewalls, you can view the status of the validation process and details about the configuration changes.

View the status of applied configurations for each firewall

View the status of the validation process for each firewall configuration in the Control Center Management Server database.

You can also view the differences between the current configuration and the proposed configuration of a firewall.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Validation Status** tab. The **Validation Status** page is displayed.

   Tip: For option definitions, press **F1**.

Result

Managed firewalls and their validation statuses are listed.

Compare impacts of proposed configuration changes for a firewall

View the differences between the current configuration and the proposed configuration of a firewall in the **Configuration Changes Details** window.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Validation Status** tab. The **Validation Status** page is displayed.

   Tip: For option definitions, press **F1**.

   If a firewall has configuration differences, a **View** button is displayed in the **Differences** column.

3) Click **View** in the row of the firewall for which you want to view these differences.

Result

The **Configuration Changes Details** window appears. This window lists the differences between the current configuration of the firewall and the proposed configuration.

View configuration status

View the status of applying changes from the Control Center Management Server database to the selected firewall or firewalls.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Configuration Status** tab. The **Configuration Status** page is displayed.

   Tip: For option definitions, press **F1**.

Result

This page displays the update status for managed firewalls.

Note: The **Configuration Status** page is also automatically displayed after you perform an apply configuration.

CHAPTER 25

Policy cleanup

Contents

Use the **Policy Cleanup** tab of the **Policy** icon to consolidate access control rules and objects. You can merge similar access control rules and objects, and delete duplicate access control rules and objects that are not currently being used.

Policy cleanup nodes

The following nodes are available in the **Policy Cleanup** tree.

- **Merge Rules Wizard** — Analyze your access control rule set and combine access control rules that have common elements in the **Merge Rules Wizard**.
- **Duplicate Rules Wizard** — Analyze your access control rule set and delete duplicate access control rules in the **Duplicate Rules Wizard**.
- **Merge Objects Wizard** — Analyze your network objects and applications (for version 8.0.0 or later firewalls) or services (for version 7.x firewalls only) and combine those objects that have common elements in the **Merge Objects Wizard**.
- **Unused Objects** — Displays a list of all the unused objects to which you have access in this configuration domain in the **Unused Objects** window. You can also double-click an object to edit it or you can delete it.

Merge access control rules with common elements

Use the **Merge Rules Wizard** to merge access control rules that have shared or common elements.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Policy Cleanup** tab.

3) Double-click the **Merge Rules Wizard** node. The **Merge Rules Wizard** is displayed.

Tip: For option definitions, press **F1**.

4) Do one of the following:

- If you have a combination of version 7.x and 8.0.0 or later firewalls that are registered to the Control Center, select the version and click **Next**.
- If you have only version 7.x or 8.0.0 or later firewalls that are registered to the Control Center, click **Next**.

Information about the number of access control rules that are candidates to be merged is displayed.

5) Click **Next**. The **Setting Criteria for Merged Rules** page is displayed.

6) Make selections on this page to determine the criteria that you will use to select access control rules to be merged.

7) Click **Next**. The candidates for merger are displayed on the **Merge Rules** page. The **Merge Rule Groups** table displays access control rule groups that share elements. The **All Rules** table displays all the access control rules.

8) In the **Merge Rule Groups** table, select the access control rule or rules to be merged by selecting the **Use** checkbox. When you do this, several things occur:

- The group header color changes from grey to green, indicating that this access control rule group will be merged.
- The common element column color changes to red. Also, the data in this column now includes all the common elements that are targeted to be merged.
- The text of the access control rule that you selected now has text that is struck through.
- A new row is inserted at the top of the access control rule group with the same number as the access control rule that you had previously selected. If you select more than one access control rule in a group, the lowest selected number is displayed for this new access control rule.

9) Click **Next**. The **Results** page is displayed, which includes the totals of the changes that were made and a revised display of the access control rule set.

10) Select **Back up your Control Center Server before merging the rules**, then click **Finish** to perform the merger. A verification message appears.

11) Click **Yes** to continue or **No** to return to the wizard to make changes. Click **Back** to return to previous pages. When you get to this step again and you are satisfied with your selections, click **Yes**. A confirmation message is displayed.

12) Click **OK**. The wizard is closed.

Related tasks

Access control rule management on page 301

Delete duplicate access control rules

Use the **Duplicate Rules Wizard** to analyze your access control rules and delete duplicates.

Note: You cannot edit access control rules in this wizard.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Policy Cleanup** tab.

3) Double-click the **Duplicate Rules Wizard** node. The **Duplicate Rule Wizard** appears.

   Tip: For option definitions, press **F1**.

4) Select the version of the access control rule set to be checked for duplicates, then click **Next**.

   Access control rules are analyzed for duplication. The number of access control rules that contain duplicates are displayed on this page.

5) Do one of the following:

   - If there are no duplicate access control rules, click **Close**.
   - If there are duplicate access control rules, click **Next**. The **Delete Duplicate Rules** page appears.

6) Select the rules you want to delete, then click **Next**. The **Results** page appears. Review the access control rule set and decide if you want to proceed with deleting the selected access control rules.

7) Perform the next action as needed:

   - If there are no access control rules to be deleted, click **Close**. This is probably because you have deselected all the **Deleted** checkbox selections that were made by default.
   - To commit your changes to the Control Center Management Server, click **Finish**. Then click **Yes** to confirm the deletion. In the confirmation message, click **OK** to close the wizard.

Merge objects with common elements

Use the **Merge Objects Wizard** to analyze and combine rule objects.

The **Merge Objects Wizard** will scan your list of objects and identify the objects with common elements. You can then combine them into a single object. Only objects within the same configuration domain can be merged, unless they are in the shared domain. The shared domain object will always become the master object and the other objects will be deleted after the merge completes.

The following objects can be merged:

- Hosts
- Networks
- Address Ranges

- Net Groups
- Proxy Services
- Filter Services
- Attack Responses
- System Responses
- SMTP Application Defences
- HTTP Application Defences
- HTTPS Application Defences
- Application Defence Group

The common elements that are used to identify these objects are the same elements that are used in the retrieve process to identify similar objects that are distinguished by name only.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Policy Cleanup** tab.

3) Double-click the **Merge Objects Wizard** node. The **Merge Objects Wizard** is displayed.

   Tip: For option descriptions, press **F1**.

4) Select an object type to scan, then click **Next**. The selected object type is scanned for objects that can be merged.

   - If there are no objects that can be merged, a message appears. Click **OK** to select a different object type or to exit the wizard.
   - If there are objects that can be merged, the **Merge Objects** page appears.

5) Select the object groups to merge from the duplicate entries list.

6) For each object in the group, select an action, then click **Next**. The **Summary** page appears.

7) Review the summary information, then click **Finish**. A confirmation message is displayed, indicating that the Management Server updates have been completed and that the system will refresh all the data.

8) Click **OK**.

Result

The objects are merged and the **Merge Objects Wizard** is closed.

Manage unused objects

Use the **Unused Objects** window to display and remove objects that are not currently in use.

Steps

1) In the navigation bar, select **Policy**.

2) Click the **Policy Cleanup** tab.

3) Double-click the **Unused Objects** node. The **Unused Objects** window is displayed.

   Tip: For option descriptions, press **F1**.

4) Specify an object type, then click **Generate**. The list of unused objects appears.

   Note: The more objects you include in the filter, the longer the report will take to generate.

5) Delete any unnecessary objects, then click **Close**.

Result

Objects deleted from the **Unused Objects** window are removed from the Management Server and no longer appear in the policy trees.

PART III

Dashboards

Contents

Control Center dashboards provide quick insight into the status of your network and managed firewalls.

CHAPTER 26

Dashboards icon

Contents

The **Dashboards** icon consists of different pages of information that quickly allow you to monitor the status of the Control Center Management Server and any of the firewalls that it manages.

How the Dashboard is organized

There are several tabs are available.

- **Status** — Provides information in a graphical, easy-to-access format so that you can monitor the status of the Control Center Management Server and the firewalls that it manages.
  In additional to the data that is displayed on this page, there are various links that display additional information when selected.

  The **Status** page is the default display for the Control Center Client application.
- **Summary** — Provides a summary report of Applications, Threats, Policy, Geo-location, Users, Global Threat Intelligence, and Endpoint Intelligence Agent.
  The dashboard summary page displays firewall reports under seven categories. The reports allow you to drill down data, view audit logs, reputation audits and heuristics evidence, and specific details.
- **Firewalls** — Provides a summary of the status of all the firewalls that are configured for your operation.
- **Licenses** — Displays the status of various licenses for all the firewalls.

View general information about the Control Center Management Server and firewalls

View the status of the Control Center Management Server and general information about alerts, resources, Messages from Forcepoint, and recent configuration changes.

The **Status** page is the default page that is displayed when you log on to the Control Center Client application and when you select the **Dashboards** icon.

View historical data about the Control Center Management Server

You can view historical data about the Control Center Management Server in the **Control Center Resources** window.

This data is updated on the Management Server every 30 minutes by default. By default, a cleanup operation happens every night at 3:30 AM Server time. You can change this default setting and the default refresh rate setting for the Management Server on the **Server Properties** window. Data older than the seven days is removed and data for the past seven days is retained.

For High Availability configurations, this window displays the primary and backup Control Center Management Server details. If the backup Control Center Management Server is not available, an unreachable/failed message is displayed.

To view this historical data:

Steps

1) In the navigation bar, select **Dashboards**.

2) Make sure that the **Status** tab is selected. The **Status** page is displayed.

3) In the **Control Center Resources** area, click **Control Center Resources**. The **Control Center Resources** window is displayed.

4) [Optional] Refresh the data being displayed by changing the value in the **Display data from the past <*n*> hours** field.

5) View the data as needed.

   Tip: For option descriptions, press **F1**.

6) Click **Close** to close this window.

View NIC information for the Control Center Management Server

You can view information about the network status of the interfaces on the Control Center Management Server in the **Interface Status** window.

To view this window:

Steps

1) In the navigation bar, select **Dashboards**.

2) Make sure that the **Status** tab is selected. The **Status** page is displayed.

3) In the **System Status** area, click **Interface Status**. The **Interface Status** window is displayed.

4) View the information on the tabs of this window and refresh as needed by clicking **Refresh**.

> **Tip:** For option descriptions, press **F1**.

5) Click **Close** to close this window.

View messages from Forcepoint

You can view information about the Control Center Management Server and the current version of the registered firewalls in the **Messages from Forcepoint** area. You also have the option to view messages for all product types and versions in this area.

Messages about the following types of information can be displayed:

- New software releases.
- Signature updates.
- Virus protection engine updates.
- Product end-of-life announcements.
- Critical hotfixes.
- Other critical product-related messages.

You can configure the frequency of message downloads and the target location of these downloads on the **Dashboards** tab of the **System Settings** window.

View system information

The **System Information** area of the **Status** page displays system information like hostname, version about the Control Center Management Server.

View improved category reports

Administrators can view an improved summary report of the top applications, threats, users, and source and destination Geo-Locations and IP addresses.

The dashboard summary page displays 20 firewall reports under seven categories. The reports allow you to drill down data, view audit logs, and specific details.

> **Note:** For 8.x firewalls (except 8.3.0 and later), the IPS Usage, Rule Usage, and Geo-Location Usage reports can be generated from **Monitor** > **Reports**. From 8.3.0 onwards, these reports can be generated from **Dashboard** > **Summary**.

Benefits of summary report include better operation, use in forensics, and ease of use. The category reports have pre-filters that enable you to select a variable and view corresponding audits.

You can configure the rows of data, time period, and the number of top elements you wish to view in the report. You can also export the report data to a Microsoft spreadsheet.

Steps

1) In the navigation bar, click **Dashboards** > **Summary**.
   The **Summary** page is displayed.

2) Use the drop-down menus to configure the view for the category reports.
   - **Display the** — Select the number of rows you want to view in the report. By default, this value is **Top 15**.
   - **from** — Select the firewall for which you want to generate the report.
   - **over the** — Select the time period. You can view data for the past 180 days.

3) Select the firewall report you want to view from these categories.
   - **Applications**
     - Network Applications
     - Network Application Categories
     - Host Applications
   - **Threats**
     - Protocol Violations
     - IPS Events
     - Virus Events
   - **Policy**
     - Access Control Rules
   - **Geo-Location**
     - Destination IPs
     - Destination Countries
     - Source IPs
     - Source Countries
   - **Users**
     - Users
   - **GTI**
     - Network Applications
     - Destination IPs
     - Destination Countries
     - Source IPs
     - Source Countries
     - Users
     - Executable
     - Malicious Executable
   - **EIA**
     - Host Application Reputation
     - Malicious Host Application Reputation

4) Click **Go**.
   The selected reports are displayed.

5) Click **Export** to export the report in an excel format. Click **View Audit** to view the corresponding audit for the report.

Note: **View Audit** option is not available for **Applications | Network Application Categories** and **Threats |Virus Events** reports.

Tip: From **EIA**, use **View Reputation Audits for user** and **View Reputation Audits** to view Endpoint Intelligence Agent related audit entries.

View the overall status of your firewalls

You can monitor the status of the firewalls that your Control Center Management Server manages in a graphical format on the **Firewalls** page.

Although this information can help you to determine operational information about the individual firewalls that are distributed throughout your system, this is only one of several different windows and pages that you can use to evaluate the status of your security system against the requirements of your security policy.

To view information about the firewalls:

Steps

1) In the navigation bar, select **Dashboards**.

2) Click the **Firewalls** tab. The **Firewalls** page is displayed.

3) View the information on this window and refresh as needed by clicking **Update Status**.

Tip: For option descriptions, press **F1**.

Firewall license reports

The functions and capabilities of each firewall are controlled by the installed licenses. You can generate the license report and view the results for all firewalls on the **Licenses** page.

View the status of all the licenses for a firewall

You can view license information for all the firewalls that are managed by the Control Center Management Server on the **Licenses** page.

You can also filter the display for an imminent expiration timeframe (as in, only show those licenses that expire in the next 30 days). Additionally, you can view the actual license information for any selected firewall on the **Firewall License** window.

To view the status of the licenses on your firewalls:

Steps

1) In the navigation bar, select **Dashboards**.

2) Click the **Licenses** tab. The **Licenses** page is displayed.

3) Change the column sort order and adjust the expiration timeframe as needed.

   Tip: For option descriptions, press **F1**.

4) (Optional) View specific license information for a firewall by selecting it in the list and clicking **View License**. The **Firewall License** window is displayed. Make changes as needed and click **OK** or **Cancel** to return to the **Licenses** page.

5) (Optional) To print this report or prepare to print this report, click **Print** or **Print Preview**, respectively.

Related tasks

View and manage firewall licenses on page 430

PART IV

Monitoring

Contents

View and identify events and responses on managed firewalls.

CHAPTER 27

Monitor icon

Contents

The **Monitor** icon presents information about customized actions that occur when specific conditions occur on an associated firewall.

About the Monitor icon

Monitoring firewall activity is important so that you can detect and respond to threats and critical conditions. You can configure the firewall to recognize unusual or abnormal occurrences and customize your response to these events.

The following tabs are available in the **Monitor** icon:

- **Alerts** — Select this tab to view the alerts to detect and respond to threats.
- **Firewall Audit** — Select this tab to view the **Firewall Audit** page, in which you can select parameters to generate a report of all the audit events for one or more firewalls.
- **Reports** — Select this tab to view a menu that allows you to select an option to generate a report for one or more firewalls. The following reports are available:
  - **Rule Usage** — [Available only for firewall versions 8.0.0 or later] Select this option to configure and view the **Rule Usage** page, in which you can view a summary of the most often used access control rule, the least often used access control rule, and access control rules that are not used by any firewall. There are various options that you must select in the **Rule Usage** window before you can generate this report.
  - **Change Report** — Select this option to configure and view the **Change Report** window, in which you can select parameters to generate a report about the changes that were made to an object that was applied to a firewall or cluster. You must select a firewall before selecting this menu option and this report function must be enabled in the **System Settings** window.
  - **Policy Report** — Select this option to view the **Policy Report** window, in which you can select parameters to generate a report about the security policy that has been defined and implemented on the selected firewall.
  - **Firewall Syslog** — Select this option to view the Firewall Syslog window, in which you can view, analyze, and manage raw data from a firewall.
  - **Firewall Reports** — Select this option to display a submenu from which you can select a firewall-specific report to generate for one or more firewalls.
- **Packet Capture** — Select this tab to display the **Packet Capture** page, in which you can configure, start, stop, and view (by using third-party software) packet data.
- **Compliance Status** — Select this tab to display the **Compliance Status** page, in which you can view all the managed firewalls and status information for all the firewalls in your configuration that are managed with the Control Center.

Tip: When you have multiple clients running simultaneously and different user permissions to manage firewalls, you might be unable to dynamically view details on a tab. Press **F5** on the specific tab or go to a different tab and revert to the tab. This refreshes the tab information and displays the updated details.

Related concepts

Troubleshooting network status using packet captures on page 532

CHAPTER 28

Alerts

Contents

The alert management functions and operations form the foundation of this dashboard feature. The primary focus of this feature is to identify alerts and use various interfaces and reports to investigate the causes and to correct the conditions of multiple firewalls from a central location.

Working of alerts

Monitoring firewall activity is important so that you can detect and respond to threats and critical conditions. The firewall can be configured to recognize unusual or abnormal occurrences, and the response to these events can be customized. These types of events are referred to as *alerts*.

Alerting is the process of detecting, recording, and notifying firewall administrative personnel of unusual or abnormal events observed during real-time monitoring of the firewall audit trail. Alerts help administrators to:

- Monitor problem areas of the system.
- Fix small problems before they become large problems.
- Counter security attacks.

Alerts operate by monitoring the auditing logs for the occurrence of specific, abnormal conditions and by building a customized response. For example, if a virus is detected, the firewall can send an email to the administrator and run a command to stop the virus.

When you click the **Alerts** tab on the **Monitor** icon, the **Alerts** page is displayed.

Related tasks

Manage alerts on page 394

Investigating alerts

Often, the root cause of an alert is obvious as indicated by the content of the associated message. However, for those alerts that have been generated when the root cause or the corrective action is not self-evident, you can use the other resources in the Control Center to investigate the cause and to correct the condition that generated the alert.

You can accomplish the following tasks about alerts:

- **Browse alerts** — The **Alerts** page provides a summary of firewall-generated alerts. Use this page to perform the following tasks:
  - Visually examine a summary of each alert.
  - Sort and manage how the alerts are displayed.
  - Acknowledge alerts.
  - Unacknowledge, annotate and review the actions that are taken for each alert.
  - Review alert messages.
  - Determine the time at which an alert occurred so that you can investigate the activities that were logged when the alert occurred.
- **Evaluate the status of the Secure Alerts Server** — An integrated Secure Alerts Server collects the alerts, activities, and events that are generated by the supported firewalls, it normalizes the data, and it stores the data in the Secure Alerts Server database. This data becomes the source for the information that is displayed on the **Alerts** page. Use the **Secure Alerts Server Status** page to view the status of the associated server.

Column data

This table lists the definitions for the various column headings when you are viewing alerts and events in the **Monitor** icon. Each row in this table specifies the name that is used for the column heading, the view of the data that supports the heading entry, and a definition of the heading content. You can view these columns on the **Alerts** page.

Table 34: Column heading definitions

Column heading name	Description
Ack	Select this checkbox to acknowledge the associated alert. When an alert is acknowledged, you must annotate the alert record by using the **Alerts** page. **Tip:** You can also unacknowledge alerts. The Alert status changes to **Open** status.
Id	Unique alert identifier assigned by the Secure Alerts Server.
Status	Current status of the alert. The available values are: **Open**, **Cleared** or **Acknowledged**.
Priority	Priority that is assigned to the alert. There are five levels of priority, listed below from the highest value to the lowest value: • **Red** — Critical • **Orange** — High • **Yellow** — Low • **Green** — Warning • **Transparent** — Information
Name	Name of the alert as defined by the sending firewall and the Management Server.
Event Type	Type of event as defined by the sending firewall and the Management Server.
Count	Number of alerts of this class for a specific firewall and Management Server.
Processing Rule	Name of the alert processing rule.

Column heading name	Description
Alarm	Name of the alert alarm.
Alarm Sound	Name of the alarm sound.
Device Id	Identification of the firewall and Management Server.
Device Name	Name that was assigned to the specific firewall when the firewall was configured or Local CC Server to represent the Management Server.
Device Address	Dotted decimal IP address for the firewall and Management Server.
Device Type	Type of the firewall and Management Server.
Acknowledge Count	Number of alerts that were acknowledged.
Annotation	Annotation message for that alert.
Reason	Information in the reason field for the alert.
Source Address	Dotted decimal IP address of the originating node for the specific alert (if known).
Source Zone	Associated source zone that is in use for the specific alert (if known).
Source Port	Associated source port number that is in use for the specific alert (if known).
Destination Address	Dotted decimal IP address of the destination node for the specific alert (if known).
Destination Zone	Associated destination zone that is in use for the specific alert (if known).
Destination Port	Associated destination port number that is in use for the specific alert (if known).
Attack Address	Dotted decimal IP address of the attack node for the specified alert (if known).
Protocol	Associated protocol that is in use for the specific alert (if known).
Interface	Associated interface that is in use for the specified alert (if known).
User	Associated user name for the specific alert (if known).
Message	Associated message for the specific alert (if known).
Description	Description of the alert.
Duration	Time, in milliseconds, between the First Time and Last Time.
Start Time	Time stamp for the first time that the alert was generated from the perspective of the local clock for the Secure Alerts Server.
Stop Time	Time stamp for the last time that the alert was generated from the perspective of the local clock for the Secure Alerts Server.
Acknowledge Time	Time stamp of the time that the alert was acknowledged from the perspective of the local clock for the Secure Alerts Server.
Closed Time	Time stamp that reflects the time at which the alert was closed.
Last Update Time	Time stamp that reflects the time at which the alert was last updated.

Map sound files to alarms

You can select the sound that is mapped to the specified alarm sound. You can specify up to five different alarm sound options (1-5) and each one can be loaded with a sound file of your choice.

Steps

1) In the main toolbar, select **Monitor**.

2) Click the **Alerts** tab. The **Alerts** page is displayed.

3) Click **Options** > **Sound Options** from the toolbar. The **Alarm Sound Mappings** window is displayed.

   Tip: For option descriptions, press **F1**.

4) In the area for the alarm sound that you are mapping, click **Use Default** or **Specify**.

5) If you selected **Use Default**, skip to Step 7.
   If you selected **Specify**, specify the name of the alternate sound file.
   Click **Browse** to locate the desired sound file.

6) When you find the file, double-click it to insert the value into the **Specify** field.

7) Click **OK** to save your changes.

Manage alerts

The **Alerts** page provides a summary of firewall-generated alerts that have been configured to send alerts to the Secure Alerts Server.

Use the **Alerts** page to visually examine a summary of each alert, sort and manage how the alerts are displayed, acknowledge and clear alerts, annotate and review actions taken for each alert, review alert messages, and determine the time at which an alert occurred so that you can investigate the activities that were logged during the same period of time.

Each alert that is displayed on the **Alerts** page represents a summary of similar events that are generated by the same firewall. The number of similar events is displayed in the **Count** field.

Use the **View Event in Audit** option to view the associated audit.

The main objective of the **Alerts** page is to quickly identify the alerts that are being generated by the configured firewalls, acknowledge them, annotate the corrective actions that are taken, resolve the problem, and clear the alert.

Several interfaces are available to investigate and clear alerts. To help you understand how to manage alerts, you must first understand that alerts have three states:

- **Open** — These are new alerts that have been identified for which no action has been taken. This is the initial state of all alerts as they are generated.
- **Acknowledged** —These are alerts that have been acknowledged and that are in the process of being investigated and corrected. An alert can be acknowledged in any of the following ways:
  - Select the **Ack** checkbox on the **Alerts** page.

  - Highlight one or more alerts and click **Ack**.
- **Clear** — These alerts have been acknowledged and corrected. An alert can be closed by selecting the **Close** button on the **Alerts** page or by highlighting one or more alerts and clicking **Close**. If an open alert is closed, the alert is automatically acknowledged. When an alert is closed, a message is sent to the associated firewall to set the alert count to zero. This occurs only if the firewall is currently communicating with the Management Server.

Use **Columns** to display the **Column Selector** window. Use this window to select the columns to display on the **Alerts** page.

- For Control Center devices, click **View Event in Audit** to display the **Audit Trail** window.
- For Sidewinder devices, click **View Event in Audit** to display the **Firewall Audit** window.

Note: Audits for the last 5 minutes are displayed in these windows.

Because each alert that is displayed on the **Alerts** page represents a summary of similar alerts that are generated by the same firewall, you might have to view all the related events that are associated with an alert to determine the root cause. To view the events associated with an alert, highlight one or more alerts on the **Alerts** page by clicking the number in the first column and click **View Event in Audit**.

To investigate the cause of an alert, you can review the chronological activities that were recorded by the affected firewalls during a range of time around the time that the alert occurred. This is accomplished by noting specific information about the alert or selected alerts, such as:

- Associated firewall
- Date and time
- Source and/or destination IP address

View alerts

You can view and manage alerts on the **Alerts** page.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Alerts** tab. The **Alerts** page is displayed.

Result

Each line on the **Alerts** page represents a summary of all the similar alert events for that firewall. The number of similar alert events is indicated in the **Count** column. To view the associated events, highlight one or more alerts and click **View Event in Audit**.
You can use each column title on the **Alerts** page to sort the displayed alerts in ascending or descending order by clicking on the column headings.

Each row that is associated with an alert is color-coded to provide a visual indication of the priority of the alert. Refer to the following table of the alert priority colors:

Table 35: Alert priorities

Alert	Priority	Color
1	Critical	Red
2	High	Orange
3	Medium	Yellow
4	Low	Green
5	Warning	Pale green

The first column in the table is the row number column. Click this column to highlight an alert. To highlight more than one alert, press **Ctrl** and then click or press **Shift** and then click again.

View events for a specific alert

Access the **Alerts** page.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Alerts** tab. The **Alerts** page is displayed.

3) Select an alert by clicking the number in the first column. Click **View Event in Audit**.
   - For Control Center devices, click **View Event in Audit** to display the **Audit Trail** window.
   - For Sidewinder devices, click **View Event in Audit** to display the **Firewall Audit** window.

View additional event information

Access the **Audit Trail** or **Firewall Audit** window.

Steps

1) In navigation bar, select **Monitor**.

2) Click the **Alerts** tab. The **Alerts** page is displayed.

3) Select an alert. Click **View Event in Audit**.
   - For Control Center devices, click **View Event in Audit** to display the **Audit Trail** window.
   - For Sidewinder devices, click **View Event in Audit** to display the **Firewall Audit** window.

4) Select an object row to view details. You can set, print, export, filter the objects on these windows.

Configure columns for the Alerts page

Access the **Column Selector** window.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Alerts** tab. The **Alerts** page is displayed.

3) In the toolbar, click **Options** > **Columns**.
The **Column Selector** window is displayed.

4) Select or deselect the columns you want to view on the Alerts page.

Filter the alerts to be displayed on the Alerts page

Access the **Alert Filter** window.

Steps

1) In navigation bar, select **Monitor**.

2) Click the **Alerts** tab. The **Alerts** page is displayed.

3) Click **Filter | Status** in the toolbar. Select the alert statuses that you want to view.

4) Click **Filter | Device** in the toolbar. Select **Control Center** or **Forcepoint Sidewinder** alerts that you wish to be displayed.

5) Filter the alerts based on priority using the show / hide options.
   - Show / Hide critical priority alerts
   - Show / Hide high priority alerts
   - Show / Hide medium priority alerts
   - Show / Hide low priority alerts
   - Show / Hide warning alerts

Cleaning old alerts

When you do not clean up old alerts over a period of time, you might face performance issues like increase in Alert database size. Purgedata with a set priority can help you to clean open, orphan, and closed alerts.

Currently **Purgedata** cleans up alerts based on the settings in the `/usr/local/dcserver/conf/purgedata.properties` file as shown below. There is an additional **Priority** option that cleans all the open, orphan, and closed alerts based on the set priority.

##

Examples of possible values

```
#activealerts=1 - deletes the active alerts older then 1 day #
#activealerts=1d - deletes the active alerts older then 1 day #
#activealerts=1h - deletes the active alerts older then 1 hour #
#activealerts=never - doesn't delete the active alerts #
```

##

```
activealerts=1
orphanalerts=1
closedalerts=1
```

##

Examples of possible values with additional priority setting

```
#activealerts=1 - deletes the active alerts older then 1 day #
#activealerts=1d - deletes the active alerts older then 1 day #
#activealerts=1h - deletes the active alerts older then 1 hour #
#activealerts=never - doesn't delete the active alerts #
#priority=1 - priority of the active alerts #
```

#priority should be between 1 and 5 #

#"1-Critical", "2-High", "3-Medium", "4-Low", "5-Warning" #

##

```
activealerts=30d
priority=2
orphanalerts=1
closedalerts=1
```

The default value of priority is set to **High** and cleans up alerts that are older than 30 days. Since this is configurable, if you don’t want to clean up active alerts, you can modify this setting.

Secure Alerts Server

The Secure Alerts Server collects the configured alert and event activity that is recorded by each supported firewall, normalizes the data, and inserts it into the database that serves as the data resource for the Reporting and Monitoring Tool. This data becomes the foundation of the alerts, events, and activities that are accessed and viewed by using the various windows and pages in the Reporting and Monitoring Tool:

- **Alerts** page
- **Audit Trail** window
- **Firewall Audit** window

This data is used to perform the following tasks:

- Reconstruct system events.
- Deter improper system use.
- Assess and recover from damage.
- Monitor problem areas.
- Capture relevant information about system events.
- Assign accountability.

In the initial release of the Secure Alerts Server, you can view the status of the server and its service history.

Functions of the Secure Alerts Server

These steps describe the basic operation of the Secure Alerts Server.

To begin, the firewall must be added to the Control Center configuration by using the Client application.

Each supported firewall must be individually configured to log events and activities to the Secure Alerts Server. You can configure the events that are logged so that you can tune your environment to report only those security events that make the most sense for your configuration.

1) The configured events and activities are sent to the Secure Alerts Server. The Secure Alerts Server normalizes the data and stores it in the Secure Alerts Server database. This database provides the storage foundation for all firewall events and activities collected from all the respective firewalls that are supported by the Secure Alerts Server.

2) After the normalized data is inserted into the database, it becomes immediately available to the Management Server and the Client application.

3) The Client application retrieves the security events from the Management Server.

You can use several interfaces to manage the subsequent data. The following interfaces are available:

- Alerts page
- Audit Trail window
- Firewall Audit window

View Secure Alerts Server status information

Access the Secure Alerts Servers page.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Alerts** tab.

3) Click **Secure Alert Server Status**.
The **Secure Alerts Server Status** window is displayed.

CHAPTER 29

Firewall audit

Contents

The auditing feature provides a series of auditing reports containing audit records for single or multiple firewalls.

Firewall audit data management

Audit reports are generated from the data that is collected in the audit log files for each firewall in your configuration.

To enable an audit report to be generated on the Control Center icon, the audit archive files or encrypted audit archive files from each firewall must be placed in defined locations on the Control Center Management Server.

Note: Do not confuse the security firewall-specific audit data with the Control Center audit trail that provides a record of actions that are performed by Control Center users.

The Management Server contains a base directory in which all audit data is stored. Within this base directory, a directory is created for each firewall that is being managed by the Control Center. The audit archive files are placed in the directory that corresponds to the Control Center on which they were generated. Information about enabling the firewalls to place audit log data on the Management Server is provided in the **Offbox** area on the **Firewall** window in the **Policy** icon.

CAUTION: Log files grow very quickly and can consume vast amounts of disk space on the Management Server. Make sure that you manage your system resources by archiving or purging your audit log files on a regular basis. The base directory that is created on the Management Server for the log files is `/var/cc/audit/sidewinder`. A separate sub-directory is created for each firewall object that is created in your configuration.

Firewall audit content

Each audit report consists of a chronologically ordered sequence of audit records for a single firewall or multiple firewalls over a user-specified period of time.

Each audit record is a standardized representation of an audit event. Audit events are notable occurrences in network traffic and system activity on the appliance. For example, an audit event records when a network session is terminated, an infected file is discovered, or a new process is created.

The audit reports that are created from the log files are highly configurable and offer the flexibility to be customized to obtain reports that provide the most useful information for your organization and network configuration.

To view details about a particular event in the audit report, you can double-click that event in the **Firewall Audit** page. The **Firewall Audit Event Viewer** window is displayed, in which you view the details of this event and you can also view other events by using the **Previous** and **Next** buttons.

Although the audit reports generated by firewalls are different and the foundation data from which the reports are derived is different, they both can be useful tools that can be used to perform many different functions.

Related concepts

About data management of Control Center audit on page 521

Managing firewall audit data

The **Firewall Audit** tab of the **Monitor icon** of the Control Center Client application is used to view audit data for one or more firewalls. You can also view detailed audit event information about a single event.

You can also configure the color schemes on the **Firewall Audit** page.

Configure and generate audit data for one or more firewalls

Access the **Firewall Audit** page to configure and generate firewall audit data.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Firewall Audit** tab. The **Firewall Audit** page is displayed.

3) In the Filter area, enter a filter criteria or select a pre-generated filter using **Filters**.

4) From the **Select time range** drop-down list, select **Custom Time Range** or **Predefined time range** to generate a historical audit or **Real Time** to generate a real time audit.

5) In the **Select audit source** options, select a managed firewall or imported audit for generating a report.

6) Click **Generate Audit**.
   A historical or real time audit report is generated.

7) View the generated audit report for details like priority of events, source and destination IP addresses, zones, and ports, application, and type code that identifies the type of problem.

8) Click **Export** to save an audit file.

9) [Conditional] Click **Get Evidence** to view firewall audit entries related to Endpoint Intelligence Agent.
   For more details see section, *View reputation specific firewall audits*.

Related tasks

View reputation specific firewall audits on page 224

Pre-defined filters and event types

Use the following tables to view lists of predefined filters and descriptions of the event types that each filter audits.

Table 36: Common predefined audit filters

Audit filters	Description
All Audit	Detects all attack and system events, regardless of type.
Attack All	Detects attack events of all severities. This option also 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 configuration of the firewall changes.
System All	Detects the system events of all severities, including power failures, hardware and software failures, failover events, license expiration, host license exceeded, log overflows, and IPsec errors.
GTI	Detects attacks identified as spam by McAfee Global Threat Intelligence.
VPN	Detects VPN audit events.

Table 37: Advanced predefined audit filters

Audit types	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.
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. Severe attacks indicate that something is occurring that an administrator should know.
Attack Severe	Detects severe attacks. This option also detects severe Application Defense violation attacks, buffer overflow attacks, DOS attacks, general attacks, policy violation attacks, protocol violation attacks, virus attacks, and spam attacks.
Buffer Overflow Attack	Detects attempted buffer overflow attacks targeted at systems protected by the firewall.
Denied Authentication	Detects when a user attempts to authenticate and specifies invalid data. For example, if a user is required to specify a password and specified it incorrectly, the denied auth event would log the event.

Audit types	Description
DOS All	Detects Denial of Service attacks of all severities. This attack category also detects all severities of TCP SYN attacks and proxy flood attacks.
DOS Severe	Detects severe Denial of Service attacks. This attack category also detects TCP SYN attacks and proxy flood attacks. Severe attacks indicate that something is occurring about which an administrator should know.
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.
General Attack Severe	Detects severe general attacks that do not fall into the predefined categories. Severe attacks indicate that something is occurring about which an administrator should know.
HA Failover	Detects when a failover IP address changes because a High Availability cluster failed over to its secondary/standby.
Hardware Software Failure	Detects some hardware failures, such as RAID, hard drive, and AMIR monitor failures.
Host License Exceeded	Detects when the number of hosts protected by the firewall exceeds the number of licensed hosts.
Hot Process	Detects the hot processes (processes that consume too much CPU or memory) events. Filter expression is `type AUDIT_T_HOT_PROCESS`.
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 mail 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 a malicious executable sending traffic through the firewall. Filter expression is `event AUDIT_R_FILEREP_MALWARE`.
Network Probe	Detects network probe (netprobe) attacks, which occur any time that a user attempts to connect or send a message to a TCP or UDP port when the security policy does not include a service that is expecting to receive traffic on that port. **Note:** The firewall does not blackhole netprobe attacks because they are likely to be Denial of Service attacks from spoofed source addresses.
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. This attack category also detects all severities of failed authentication attacks, ACL and IP filter deny attacks, and Type Enforcement error attacks.

Audit types	Description
Policy Violation Severe	Detects severe attacks that violate the active policy. This attack category also detects failed authentication attacks, ACL and IP filter deny attacks, and Type Enforcement error attacks. Severe attacks indicate that something is occurring about which an administrator should know.
Power Failure	Detects that a UPS power failure occurred.
Protocol Violation All	Detects attacks of all severities that violate protocol compliance.
Protocol Violation Severe	Detects severe attacks that violate proxy protocols (HTTP, Telnet, FTP, and so on). Severe attacks indicate that something is occurring about which an administrator should know.
Proxy Flood	Detects potential connection attack attempts. A connection attack is defined as one or more addresses that launch 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.
Signature IPS Intrusion All	Detects all attacks that are identified by the signature-based IPS. This category detects attacks that were denied, dropped, or rejected, as well as suspected attacks that were allowed, but were audited by IPS.
Signature IPS Intrusion Blackholed	Detects attacks that are identified by the signature-based IPS where the attacker was blackholed.
Signature IPS Intrusion Deny	Detects attacks that are identified by the signature-based IPS where the offending network session was dropped or rejected, or the attacker was blackholed.
Spam	Detects attacks of all severities that are spam.
Spam Severe	Detects severe attacks that are spam.
Syslog	Detects all audit attacks and system events that were created via syslog.
System Critical	Detects all critical system events, including power failures, hardware failures, critical software failures, and failover events. 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.
System Critical And Severe	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. 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 that something is occurring about which an administrator should know.
TCP SYN Attack	Detects a possible attempt to overrun the firewall with connection attempts.
Type Enforcement	Detects when there is a Type Enforcement violation because an unauthorized user or process attempted to perform an illegal operation.
Unlisted Executable	Detects unknown executable activity in the network and notifies the firewall. Filter expression is `event AUDIT_R_FILEREP_UNLISTED`.
UPS System Shutdown	Detects when UPS has directed the firewall to shut itself down.
Virus	Detects attacks of all severities that are viruses.

Audit types	Description
Virus Severe	Detects severe attacks that are viruses.

View event-specific firewall audit information

Access the **Firewall Audit Event Viewer** window.

Steps

1) In the navigation bar, select **Monitor**.
2) Click the **Firewall Audit** tab. The **Firewall Audit** page is displayed.
3) Select your report parameters and filters and click **Generate Audit**. The report data is generated.
4) Double-click the row of the audit event for which you want to view more information. The **Firewall Audit Event Viewer** window is displayed for this event.
5) [Conditional] For an EIA audit, double-click **Host_evidence** or **Host_heuristic** to display the **EIA Heuristic Report Viewer** window and view the heuristic details.

   For more details see section, *View reputation specific firewall audits*.

Related tasks

View reputation specific firewall audits on page 224

View real-time audit from the firewalls

Administrators can view real-time audit from one or multiple firewalls. A maximum of eight firewalls can be selected to view real-time audit.

Before you begin

The selected firewall must be registered with Control Center.

Use the filters on the **Firewall Audit** window to filter the real-time data. You can view and export the audits.

Steps

1) In the navigation bar, select **Monitor**.
2) Click **Firewall Audit**.
3) Under **Select audit source**, click **Managed firewall** and select one or more firewalls.
4) From the **Select time range** drop-down menu, select **Real Time**.

5) Select a filter to view the firewall audits.
   - Click **Pre-generated** to select a pre-generated audit filter.
   - Click **User-generated** to select a custom filter.

6) Click **Start**.

   The real-time audit for the selected firewalls is displayed in pages. Use the pagination buttons to navigate through the audit pages.

   Note: Two client applications cannot view real time audit from same set of firewalls (one or more) simultaneously.

   Note: Click **Stop** to stop viewing the real-time audit.

   Tip: You can stop real-time audit and sort the audit only on the **Time** column.

7) Click **Export** to save the firewall audit in XML, text, or SEF format.

Create customized color settings for the data in the Firewall Audit page

This procedure assumes that you have already generated audit data on the **Firewall Audit** page.

Steps

1) On the **Firewall Audit** page, click **Settings**. The **Firewall Audit: Color Settings** window is displayed.

2) Select **Custom**.

3) Click the table cell for the background color or text color for the severity type to modify. The **Color** window is displayed.

4) Select a basic color or click **Define Custom Colors >>** to create a custom color.

5) If you are selecting a basic color, go to the next step. or For a custom color, click in the color display on the right for the color to add. You can also move the slider up or down to adjust the settings of this selection. When you see that the color that you want is displayed in the **Color|Solid** box, click **Add to Custom Colors**.

6) Click **OK**.

7) Repeat Steps 3—6 for each table cell to edit.

8) When you have finished, click **OK** to update the **Firewall Audit** page with these color settings changes.

Configure filters for audit data

You can use predefined filters or create your own filters to filter the audit data that is displayed on the **Firewall Audit** page. By filtering the audit data, you can respond to audit events of particular interest to your site in an effective way.

To view a list of user-defined audit filters, in the **Rule Objects** tab of the **Policy** icon, click **Audit Filters** in the tree.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Firewall Audit** tab. The **Firewall Audit** page is displayed.

3) Click the **Create Filter** tab. The **Audit Filter** window is displayed.

   Tip: For a custom application filter, define the expression with no spaces and limit only to 120 character length.

4) Enter details like name and description for the audit filter.

5) In **Characteristics**, define the type of filter and SNMP trap number.

6) You can select any of available filters and narrow down a filter by source and destination zones and IP addresses.

7) Use the **Extra Criteria** area to specify additional criteria for filtering audit data.

8) Click **OK** to save the audit filter.

Filter syntax

Use the following syntax when building expressions:

- Identify a filter by using either single quotes (') or double quotes ("). All examples shown below use single quotes.
- Express “and” using either `and` or &&.
- Express “or” using either `or` or `||`.
- Express "not" using either `not` or `!`.

A filter should include the following components:

- The *type* or *facility* to search for, using one of these formats:
  - The Name format (AUDIT_T_*TYPE* as in AUDIT_T_ATTACK, AUDIT_F_*FACILITY* as in AUDIT_F_LOGIN)
  - The Short Message format (attack, login)
  - The 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:

```
(facility ping_proxy) and (src_ip 10.69.101.34 or src_ip 10.69.101.36)
```

returns this audit record:

```
Aug 22 02:02:20 2008 CDT f_ping_proxy a_proxy t_nettraffic p_majorpid: 3728 ruid: 0 euid: 0 pgid:
 3728 logid: 0 cmd: 'pingp'domain: Ping edomain: Ping hostname: mixer.ext.b.test event: proxy traffic
 end service_name: ping netsessid: 48ad640e000e0151 srcip: 10.69.101.34 srczone: internal protocol:
 1 dstip: 10.66.6.22 dstzone: external bytes_written_to_client: 83079240 bytes_written_to_server:
 83087396 acl_id: Internet Services cache_hit: 1 request_status: 0 start_time: Thu Aug 21 07:48:14
 2008
```

A source IP address of 10.69.101.34 that uses the Ping Proxy facility matches the filter expression.

CHAPTER 30

Reports

Contents

Control Center can generate more than 70 different reports.

About reports

Most of the reports are accessible from the **Reports** tab on the **Monitor** icon.

The following reports are available on this tab:

- **Rule Usage** — [Available only for firewall versions 8.0.0 or later] Select this option to configure and view the **Rule Usage** page, in which you can view a summary of the most often used access control rule, the least often used access control rule, and access control rules that are not used by any firewall. There are various options that you must select in the **Rule Usage** window before you can generate this report.
- **Change Report** — Select this option to configure and view the **Change Report** window, in which you can view information about the changes that were made to an object that was applied to a firewall or cluster. You must select a firewall before selecting this menu option and this report function must be enabled in the **System Settings** window.
- **Policy Report** — Select this option to view the **Policy Report** window, in which you can select parameters to generate a report about the security policy that has been defined and implemented on the selected firewall.
- **Firewall Syslog** — Select this option to view the Firewall Syslog window, in which you can view, analyze, and manage raw data from a firewall.
- **Firewall Reports** — Select this option to display a submenu from which you can select a firewall-specific report to generate for one or more firewalls.

Firewall access control Rule Usage reports

You can monitor the most often used access control rules, the least often used access control rules, and the unused access control rules at the firewall or group of firewalls level by generating rule use reports.

The data in these reports will assist you in managing your access control rules across your network.

Note: Rule Usage reports are available only for firewall version 8.0.0 or later.

Note: For 8.3.1 firewalls and later, the Rule Usage reports can be generated from **Dashboard** > **Summary** and **Monitor** > **Reports**.

View access control rule statistics

You can manage the effectiveness of your access control rules on one or more firewalls by running the **Rule Usage** report and viewing the results.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Reports** tab.

3) Select **Rule Usage**. The **Rule Usage** window is displayed.

4) Configure the settings and select **Wait for Report** or **Schedule Report** if you are not immediately generating the report. Note that you must also specify an email address in the **Email Address** field if you select the **Schedule Report** checkbox.

5) Your next step depends on the checkbox that you selected.
   - If you selected the **Wait for Report** checkbox, click **Request Report**. The page is displayed in the work area.

     Note: If you select multiple firewalls for this report, you must wait for it.

   - If you selected the **Schedule Report** checkbox:

   a) Specify date and time information and an email address to send the report to.

   b) Click **Schedule Report**.
      After the report has been run at the scheduled time, the report is emailed to the address provided.

Firewall change reports

You can monitor all the configuration changes that have been made at the firewall or cluster level by generating change reports.

View the changes made to one or more firewalls or clusters

The **Change Report** page is used to view all the configuration changes that were made to an object that was applied to one or more selected firewalls and clusters. This report provides the "who, what, where, when" information to the administrator so that he or she can more closely monitor the configuration changes that are being made to their firewalls and clusters.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Reports** tab.

3) Select **Change Report**. The **Change Report** window is displayed.

   > **Note:** You must select a firewall before selecting this menu option and this report function must be enabled in the **System Settings** window.

4) Configure the settings and select **Wait for Report** or **Schedule Report** if you are not immediately generating the report. Note that you must also specify an email address in the **Email Address** field if you select the **Schedule Report** checkbox.

5) Your next step depends on the checkbox that you selected.

   - If you selected the **Wait for Report** checkbox, click **Request Report**. The page is displayed in the work area

     > **Note:** If you select multiple firewalls for this report, you must wait for it.

   - If you selected the **Schedule Report** checkbox, you must specify an email address in the **Email Address** field in addition to all the date and time information. Click **Schedule Report**. This window is closed and the email of this report is sent to the addressee after the report has been run at the scheduled time

Firewall policy reports

You can view the security policy that has been defined and implemented on the selected firewall by generating policy reports.

There are two aspects to the policy report:

1) You must select the criteria for the report on the **Policy Report** window.

2) Run the report and view the results on the **Policy Report** page.

View information about the security policy for firewalls

The **Policy Report** page is used to view the security policy that has been defined and implemented.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Reports** tab.

3) Select **Policy Report**. The **Policy Report** window is displayed.

4) Configure the settings and select **Wait for Report** or **Schedule Report** if you are not immediately generating the report. Note that you must also specify an email address in the **Email Address** field if you select the **Schedule Report** checkbox.

5) Do one of the following:

   - If you selected the **Wait for Report** checkbox, click **Request Report**. The page is displayed in the work area.

     Note: If you select multiple firewalls for this report, you must wait for it.

   - If you selected the **Schedule Report** checkbox, you must specify an email address in the Email Address field in addition to all the date and time information. Click **Schedule Report**. This window is closed and the email of this report is sent to the addressee after the report has been run at the scheduled time.

Firewall reports

The Control Center **Monitor** icon has an interface to request a wide variety of firewall-specific reports. Although some firewalls share similar reports, each firewall can generate unique reports that provide insight into its operation and configuration.

Firewall report results

After selecting the report to generate, the window for the specific report is displayed. Depending on the report, this window can contain several fields. You can also choose between waiting for the report to be generated or initiating the report for asynchronous viewing (whereby you can request the report and have the results sent to an email address that you specify).

Generating aggregate reports

You can generate aggregate reports for many of the reports that are submenu options of the **Firewall Reports** menu option.

To view this list of reports, select the **Monitor** icon. Then click the **Reports** tab and select **Firewall Reports**.

After you select the report menu option, a report window is displayed with the name of the selected report in the title bar. At this point, you can determine whether this report is an aggregate report by clicking the down arrow in the **Firewall** field to display the list of firewalls. If you see checkboxes that can be used to select multiple firewalls, this is an aggregate report. If you do not see any checkboxes, this is an interactive, firewall-specific report. An example of an aggregate report is the **Blackholed IPs** report.

View firewall report data

Some reports have report-specific parameters and options that can be specified when you request a report. The name of this page will be the name of menu option that you select from the **Firewall Reports** menu on the **Reports** tab.

For example, if you select the **Running Processes** option, the **Running Processes** window is displayed, in which you specify your report parameters. When the report is generated, the **Running Processes** page is displayed.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Reports** tab.

3) Select **Firewall Reports** and then select the name of the report to generate. The report window is displayed.

4) Specify the options on the report window. Click **Request Report**. The report page is displayed.

Firewall Report pages

Some reports have report-specific parameters and options that can be specified when you request a report.

The name of this page will be the name of menu option that you select from the **Firewall Reports** menu on the **Reports** tab. For example, if you select the **Running Processes** option, the **Running Processes** window is displayed, in which you specify your report parameters. When the report is generated, the **Running Processes** page is displayed.

Firewall report summaries

Use the following summary description of the firewall reports and their associated report parameters (if any) to determine the report or reports to generate.

Table 38: Reports and associated parameters

Report name	Description and optional parameters
Active Internet Connections	This report displays information about active Internet connections, including the protocol, the receive and send queue size (in bytes), local and foreign addresses, and the internal state of the protocol. Report presentation is by Protocol, Recv-Q, Send-Q, Bu, Local Address, Foreign Address, and State. • **Include Servers** — When selected, displays the state of all sockets, including those that are used by server processes. • **Do not resolve names** — When selected, displays IP addresses, rather than host and domain names. Name resolution can be time-consuming. If there are network problems (for example, if the DNS server is unavailable), name resolution can take a long time.

Report name	Description and optional parameters
Antivirus Patch Version Information	This report displays information about the current virus protection engine version number for the selected firewall. Report presentation is by Name and Value.
Application Signatures Database Version	[Available only for firewalls version 8.0.0 or later] This report displays information about the current database version number of the application signatures database file for the selected firewall. Report presentation is by Name and Value.
Application Usage	[Available only for firewalls version 8.0.0 or later] This report displays information about the amount of activity that has been registered for applications in the selected firewall. The information is divided by most-often used and least-often used. Report presentation is by Application, Hits, and Total Bytes Last Used. • **Units** — Determines the value to use in the report. • **Number of days/hours to limit to** — Specifies the time limit for the report. • **Limit results to the top** — Specifies the maximum number of objects displayed in the report. Only the first *n* objects are displayed.
ARP Table	The Address Resolution Protocol (ARP) is a TCP/IP protocol that is used to convert an IP address into a physical address. To obtain a physical address, a host broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address. This report displays the system's Internet-to-Ethernet address translation table that is used by ARP. Report presentation is by Name, IP Address, and MAC Address. **Do Not Resolve Names** — When selected, displays IP addresses, rather than host and domain names. Name resolution can be time-consuming. If there are network problems (for example, if the DNS server is unavailable), name resolution can take a long time.
Authentication - Locked Out Users	This report displays information about the current authentication failures by user name and by the number of failures for the selected firewall. Report Presentation is by User Name and Number of Failures. Options include: • Flushing all the authentication failures • Flushing those failures for selected multiple users • Flushing only those failures for a selected individual user
Blackholed IPs	This report displays information about the suspect or untrustworthy IP addresses that have attempted to access and infiltrate the selected firewall. These IP addresses are segregated and quarantined. Report presentation is by IP, Zone (for version 8.0.0 or later firewalls), Burb (for version 7.x firewalls), and Expire Time.
Bridging Configuration and Status	This report displays information on the configuration and status of bridged interfaces. Report presentation is by Interface.

Report name	Description and optional parameters
Cluster Status	This report displays information about the network cluster for the selected firewall. Report presentation is by Node, HA Mode, IP Address, State, and Status.
Current Passport Users	This report displays information about the current users that are logged into the selected firewall by using Passport, which provides the user authentication process. Report presentation is by Name, External Group, Authenticator, IP Address, Issued, and Last Used. Options include: • Revoking all passports • Revoking passports for individual users
Disk Utilization	This report displays information about the disk space consumption for each file system for the selected firewall. Report presentation is by File System, Total Size, Used, Available, Percent Used, and Mounted On.
Enrolled Hosts	This report displays information about the current enrolled hosts for the selected firewall. The information includes the associated license type (either Limited or Unlimited) and the IP Address. Report presentation is by IP Address. Options include removing the IP host from the enrolled list.
Geo-Location Usage	[Available only for firewalls version 8.0.0 or later] This report displays information about the amount of activity that has been registered for Geo-Locations in the selected firewall. The information is divided by most-often used and least-often used. Report presentation is by Geo-Location, Hits, and Total Bytes Last Used. • **Units** — Determines the value to use in the report. • **Number of days/hours to limit to** — Specifies the time limit for the report. • **Limit results to the top** — Specifies the maximum number of objects displayed in the report. Only the first *n* objects are displayed.
Geo-Location Version	This report displays information about the Geo-Location object for the selected firewall. Report presentation is by Version.
Interface NIC Status	This report displays information about the status of each NIC or NIC group for the selected firewall. Report presentation is by Interface Name, IP Address, Zone (for version 8.0.0 or later firewalls), Burb (for version 7.x firewalls), Active NIC, Active Speed, Enabled, Up, and Connected.

Report name	Description and optional parameters
IPS Signature Usage	[Available only for firewalls version 8.0.0 or later] This report displays information about the amount of activity that has been registered for IPS signature objects in the selected firewall. The information is divided by most-often used and least-often used. Report presentation is by Signature Name, Hits, and IPS ID Last Used. • **Units** — Determines the value to use in the report. • **Number of days/hours to limit to** — Specifies the time limit for the report. • **Limit results to the top** — Specifies the maximum number of objects displayed in the report. Only the first *n* objects are displayed.
IPS Signature Version	This report displays information about the current IPS (Intrusion Prevention System) Signature file version number for the selected firewall. Report presentation is by Version.
NDP Table	The Neighbor Discovery Protocol (NDP) is a protocol in the Internet Protocol Suite used with IPv6 to determine network addresses. A neighbor is another router or host on the same link layer (Ethernet or similar network, or IPv4 or IPv6 tunnel). Routers and hosts on the network use solicitation and advertisement messages to request and communicate neighbor addresses. This report displays the results of the NDP solicitation and the neighbor addresses. Report presentation is by Neighbor, Linklayer Address, Netif, and Expire. **Do Not Resolve Names** — When selected, displays IP addresses, rather than host and domain names. Name resolution can be time-consuming. If there are network problems (for example, if the DNS server is unavailable), name resolution can take a long time.
Network Interface Configuration	This report displays information about all the initialized network interfaces for the selected firewall. Report presentation is by interface.
Network Interface Statistics	This report displays a summary of the activity on each network interface for the selected firewall. Information includes local and remote addresses, send and receive queue sizes (in bytes), protocol, and the internal state of the protocol. Report presentation is by Name, Mtu, Network, Address, Ipkts, Ierrs, Opkts, Oerrs, and Collisions.
Network Protocol Statistics	This report displays information about the network traffic that is organized by the various protocols (TCP, UDP, IP, ICMP, IGMP, and TCP Extensions) that are used by the network packets. This report also displays routing statistics. The protocol determines the following information: • The type of error checking to be used • The data compression method, if any • The way that the sending firewall will indicate that it has finished sending a message • The way that the receiving firewall will indicate that it has received a message
Quality of Service Status	This report displays information about the Quality of Service profiles and queues that are assigned to interfaces. In the Profiles section, presentation is by Name and Queues. In the Queues section, presentation is by Name, Bandwidth, Priority, and Profile.

Report name	Description and optional parameters
Routing Statistics	This report displays a summary of the routing activity for the selected firewall. See Network Protocol Statistics above.
Routing Table	This report displays the system routing table, including cloned routes for the Internet Protocol Version 4 (IPv4). The routing table displays the available routes and indicates the associated status. Each route consists of a destination host or network and a gateway to use for forwarding packets. This table displays the way that the packets are being routed. Packets that are being sent to the IP address that is named in the Destination column are actually being sent to the IP address that is displayed in the Gateway column. Report presentation is by Destination, Gateway, Flags, Refs, Use, Zone (for version 8.0.0 or later firewalls), Burb (for version 7.x firewalls), Netif, and Expire.
Running Processes	This report displays the processes that are currently running and the system resources that they are consuming for the selected firewall. Report presentation is by Process, CPU%, Process Size, and Resident Memory.
Service Status	[Available only for version 7.x firewalls] This report displays configuration and status information for all the services that are enabled on a specific firewall. Report presentation is by Status, Service, Agent, Burbs, Ports, and Active Rules. Options include: • Viewing service information • Viewing the Audit report for the last 24 hours for the selected service • Restarting or re-enabling the selected service • Temporarily disabling the selected service
SmartFilter Database Version	This report displays the timestamp for the last download attempt for and the version number of the SmartFilter database that is installed on a specific firewall. Report presentation is by Name and Value.
SmartFilter Log	This report displays SmartFilter log information for a specified firewall. There are also navigation buttons at the bottom of this report to advance by page forwards and backwards and to the top or to the bottom of the report. Report presentation is by User IP and Name, Time of Access, and URL / Response Code / Action Taken / SmartFilter Category. • **Review log from start or end** — Specifies the order in which the log data is displayed: from front-to-back (Start) or from back-to-front (End). The default value is End. • **Number of lines per page** — Specifies a value to determine the number of lines that will be displayed on each page of the report. Available values are 100, 250, and 500. The default value is 100.
SSH Known Host Associations	This report displays a list of the strong and weak trust associations that are present on the selected firewall. Report presentation is by Trust Level, IP Address, Port, Key Type, Fingerprint, Last Modified, and Key Value.

Report name	Description and optional parameters
Static Routing Status	This report displays the active status of all the IPv4 and IPv6 (if enabled on a 7.0.1 version or later firewall) routes for the selected firewall and also the failover routes if failover routes have been configured. Report presentation information varies, depending on the status (for example, a route failover has occurred). For IPv4 or IPv6 firewall routes, presentation is by Internet Destination, Gateway, Flags, Zone (for version 8.0.0 or later firewalls), Burb (for version 7.x firewalls), and Netif. For failover routes, presentation is by Route, Gateway, Zone (for version 8.0.0 or later firewalls), Burb (for version 7.x firewalls), Netif, and Status.
System Vital Statistics	This report displays the system resources and the load factor placed on them by the current system processes for the selected firewall. The Load Average information is presented by CPU, Real Memory, Virtual Memory, Disk Use, and Load Average for the last minute, 5 minutes or 15 minutes. Report presentation is by Name and Value.
VPN Status	This report displays the active status of all the VPNs for a selected firewall. Report presentation is by Name and Status.

Generate firewall reports

Use this report window to request a firewall-specific report.

Note that the title of this window changes, depending on the name of the report that you are requesting from the **Firewall Reports** menu of the **Reports** tab in the **Monitor** icon.

For example, if you select **Running Processes** from the **Firewall Reports** menu, the **Running Processes** window is displayed.

There are currently more than 70 different reports that can be generated.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Reports** tab.

3) Select **Firewall Reports** and then the name of the report to generate. The report window is displayed.

   Note: For 8.3.0 firewalls and later, the Application Usage and Geo-Location Usage reports can be generated from **Dashboard** > **Summary**.

4) From the **Firewall** drop down list, select the firewall for which you wish to generate the report. You can search for a specific firewall using **Find**.

5) Click **Request Report**.

   The firewall report is displayed. View the report and click **Close**.

   Note: In some firewall reports, you have additional options like save the reports to a location or a specified format.

View services and manage service agents

The **Service Status** page is used to view the service status report, which contains configuration and status information for all the services that are enabled on the selected firewall.

> **Note:** This page is available only for version 7.x firewalls.

This report provides the following information:

- Status of the service.
- Burbs on which the service is listening.
- Ports on which the service is accepting connections.
- Access control rules that have been configured to use the service.

In addition to this view, you can also:

- View additional information about the selected service (**Service Information** button).
- View audit data for this service (**Audit Data** button).
- Restart the service (**Restart Agent** button) — This is helpful when you have made configuration changes or when you want to troubleshoot this service.
- Temporarily disable one or more services

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Reports** tab.

3) Select **Firewall Reports** > **Service Status**. The **Service Status** window is displayed.

4) Select the firewall or firewalls for which you are running this report and any other selections on this window. Click **Request Report**. The **Status Report** page is displayed.

View details about a firewall service

Service Information window is used to view the zones and ports on which the service should be listening, along with the current status of the service. You can also check the current status of this service and perform some of the same actions that are available from the **Service Status** page.

- Display audit data for this service (**Audit Data** button).
- Restart this service (**Restart** button).
- Temporarily disable this service (**Temporarily Disable** button).

Steps

1) If the **Service Status** page is already displayed, skip to Step 5.

2) In the navigation bar, select **Monitor**.

3) Click the **Reports** tab.

4) Select **Firewall Reports** > **Service Status**. The **Service Status** window is displayed.

5) Select the firewall or firewalls for which you are running this report and any other selections on this window. Click **Request Report**. The **Service Status** page is displayed.

Result

Select a service in the report and click **Service Information**. The **Service Information** window is displayed.

CHAPTER 31

Compliance status

Contents

Compliance status ensures the firewall configuration backups stored in the database on the Management Server match the configurations on your firewalls.

View the compliance status of the current firewall configuration

View the compliance status of one or more firewalls.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Compliance Status** tab. The **Compliance Status** page is displayed.

3) Click **Refresh** to make sure that you are viewing the most recent information.

Configure compliance status settings

Generate compliance status summaries at specified times and to send the results to specified email addresses.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Compliance Status** tab. The **Compliance Status** page is displayed.

3) Click **Settings**. The **Compliance Status Settings** window is displayed.

   Tip: For option descriptions, press **F1**.

4) Enable the compliance report.

5) Specify times and email recipients for the compliance report.

6) Click **OK**.

Result

The new compliance report is sent to the specified email addresses as scheduled.

PART V
Maintenance

Contents

Use Control Center to schedule and perform maintenance tasks on managed firewalls.

CHAPTER 32

Maintenance icon overview

Contents

Use the **Maintenance** icon to manage firewall settings.

Firewall Maintenance tree

Use the nodes on the **Firewall Maintenance** tree of the **Maintenance** icon to maintain settings for multiple firewalls and security policies for a distributed homogeneous or heterogeneous configuration.

- **Device Control** — Re-initialize, restart, and provide an orderly shutdown of selected firewalls in the **Device Control** window. You can terminate active sessions and security associations for user-selected firewalls. You can also set the date and time of one or more firewalls.
- **Firewall License** — Specify and manage firewall licenses by using the **Firewall License** window.

  Note: After an upgrade, Control Center can manage only licensed firewalls.

  Tip: Prior to an upgrade, check if the firewall is licensed or after an upgrade license the firewall using the firewall cli commands.
- **Configuration Backup** — Back up and restore configurations for selected firewalls. Use the saved configuration files to restore a default firewall configuration, to maintain a version of a working configuration before you make any configuration changes, or to recover from an unexpected loss of firewall configuration data. When you are installing software updates, this feature is a convenience and a precaution.

Maintenance icon tabs

Use the tabs on the **Maintenance** icon to perform the following tasks.

- **Deployment Status** — View the enrollment status of a specific firewall.
- **Firewall Updates** — Determine the current version of software that is installed on each firewall; install, uninstall, or roll back an update; schedule an update action for a particular date and time; view the status of an update action; and view the history of previously completed update actions.
- **Store updates** — Download, manage, and store firewall software updates on the Management Server. Use the interface to identify the name of the update, the type of firewall to which the update applies, the release date, and its download status. You can also view an associated readme file.

CHAPTER 33

Firewall maintenance

Contents

Use the Control Center to schedule and perform maintenance activities such as licensing and updating firewalls, or creating configuration backups.

Device control

You can perform many actions against one or more firewalls in the **Device Control** window. You can re-initialize, restart, and provide an orderly shutdown of selected firewalls and you can terminate active sessions and security associations for user-selected firewalls.

You can also set the date and time of one or more firewalls.

Manage firewall shutdown and suspension states and other maintenance settings

Use the **Device Control** window to initiate various shutdown or suspend states on the selected firewalls and to manage other areas, such as to reset default gateways or request management control of a firewall.

Some of these options are not applicable to all supported firewall versions.

For several of these actions, you can generate a report after you click **Proceed**. The name of the report is included in the description of the control action option.

Steps

1) In the navigation bar, select **Maintenance**.

2) In the **Firewall Maintenance** tree, double-click the **Device Control** node. The **Device Control** window is displayed.

3) From **Firewalls** list, select one or more firewalls on which operations are to be performed.

4) From **Control Actions**, specify the action to be taken on the firewalls.

5) Click **Proceed** to initiate the action on selected firewalls.

Setting the date and time on a firewall

Use the **Set Date and Time** window to set the date and time on the firewalls that are selected on the **Device Control** window.

Steps

1) In the main menu, select **Maintenance**.

2) In the **Firewall Maintenance** tree, double-click the **Device Control** node. The **Device Control** window is displayed.

3) Select at least one of the firewalls in the **Firewalls** list.

4) In the **Control Actions** list, select **Set date and time** and then click **Proceed**. A warning message is displayed, indicating that the selected device or devices are about to have their date and time values reset.

5) Click **OK**. The **Set Date and Time** window is displayed.

6) Specify a date or open a calendar to select a date to assign to the firewalls.

7) Assign or specify a time to the firewalls that were selected.

8) Click **OK**.

View and manage firewall licenses

View and manage license data for a firewall in the **Firewall License** window.

Steps

1) In the navigation bar, select **Maintenance**.

2) In the **Firewall Maintenance** tree, double-click the **Firewall License** node. The **Firewall License** window is displayed.

> **Note:** After an upgrade, Control Center can manage only licensed firewalls. Prior to an upgrade, check if the firewall is licensed or after an upgrade license the firewall using the firewall cli commands.

3) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

4) Click **OK** to save this license.

Firewall configuration backup

You can retrieve a backup configuration file that is stored on the Control Center Management Server or you can restore a backup file in the **Firewall Configuration Backup** window.

You can add a description for the manual configuration backup file or files (depending on the number of firewalls that you select) that you are about to create in the **Confirm Backup** window. This window also serves as an additional confirmation to continue with the backup process.

Backing up and restoring firewall configurations

You can use the **Firewall Configuration Backup** window to perform the following actions on the configuration file for a specified firewall.

- Retrieve a backup firewall configuration file based on the current configuration of the selected firewall or firewalls and store it on the Management Server.
- Restore a backup firewall configuration file.

You can also use this window to maintain a version of a working configuration before you make any configuration changes or to recover from an unexpected loss of firewall configuration data.

Note: Save the current configuration of all firewalls *before upgrading* the software and before making changes to the configuration.

Back up a firewall configuration

Back up a configuration for one or more firewalls.

Steps

1) In the navigation bar, select **Maintenance**.

2) In the **Firewall Maintenance** tree, double-click the **Configuration Backup** node. The **Firewall Configuration Backup** window is displayed.

3) To create a backup of the configuration data for selected firewalls, select the checkbox that is associated with each firewall.

4) Click **Create Backup(s)** to store a backup copy of the firewall configuration for the selected firewalls on the Management Server. The **Confirm Backup** window is displayed.

5) You can edit the description or accept the default value. Then click **OK** to confirm this backup. A message is displayed, indicating that this request has been sent to the firewall.

   After the backup is complete, the **Description**, **Last Backup Date**, and **Last Backup By** column values are updated on this tab.

Restore a firewall configuration

Restore a firewall to a previous configuration.

Steps

1) In the navigation bar, select **Maintenance**.

2) In the **Firewall Maintenance** tree, double-click the **Configuration Backup** node. The **Firewall Configuration Backup** window is displayed.

3) Click the **Restore** tab.

4) In the **Firewall** field, select the firewall to be restored.

5) In the table, select the row of the backup to use for this restoration and click **Restore Backup**. A system warning is displayed, indicating that the restoration is about to occur. As a result of that, the firewall will be restarted and a subsequent policy mismatch can occur.

6) Click **OK**. An information message is displayed, indicating that the restore request has been sent to the firewall. After the restore is complete, the **Restore Date** column value is updated with the current information.

Confirm a configuration backup of one or more firewalls

Use the **Confirm Backup** window to add a description for the manual configuration backup file or files (depending on the number of firewalls that you select) that you are about to create.

This window also serves as an additional confirmation to continue with the backup process.

Steps

1) In the navigation bar, select **Maintenance**.

2) In the **Firewall Maintenance** tree, double-click the **Configuration Backup** node. The **Firewall Configuration Backup** window is displayed.

3) On the **Backup** tab, select the firewall or firewalls for which you want to create configuration backup files and click **Create Backup(s)**. The **Confirm Backup** window is displayed.

4) For the selected firewall, provide a description for the backup file. The default value is **Manual backup** and can be modified.

5) Click **OK**. A message is displayed indicating that the request is sent to the firewall.

Deployment status for one or more firewalls

After you have initiated the rapid enrollment of one or more firewalls by using the **Sign Up Firewalls** window, you can view the status of the enrollment process on the **Deployment Status** page.

View your firewall enrollment (deployment) status

Use the **Deployment Status** page to view the status of the enrollment process when enrollment is initiated of one or more firewalls from the Control Center Management Server.

The enrollment process is initiated by using the **Sign Up Firewalls** window.

Steps

1) In the navigation bar, select **Maintenance**.

2) Click the **Deployment Status** tab. The **Deployment Status** page is displayed.

3) View status values in **Status** that indicate the status of the enrollment process.

4) View firewall details like IP address and type.

5) View **Details** for any error that occurred during the enrollment process.

6) Click **Clear Completed** to clear rows that display `Operation completed` in the **Status** column.

Firewall software updates

Maintaining software updates to multiple firewalls in a heterogeneous environment can be a complex task. To provide the enterprise-class protection that is required by your security policies, installing and managing software updates to firewalls is not optional.

Note: If you are upgrading from one major firewall version to another, see the Migration Guide for the firewall for information specific to the upgrade.

To help simplify the process, use the **Firewall Updates** page to manage software updates for supported firewalls that are being managed by the Control Center. The following actions are available on this page:

- Determine the current software version that is installed on each supported firewall in the configuration.

- Identify firewalls that require updates.
- Select an update action to perform on selected firewalls. These actions include install, uninstall, and rollback.
- Select an available software update.
- Determine the status of the last applied update.
- View and select the update packages to be installed, uninstalled, or rolled back and view the historical data that is associated with previous update actions.

Related tasks

Install, uninstall, or roll back software updates on page 434

Install, uninstall, or roll back software updates

You can install, uninstall, or roll back updates for one or more selected firewalls.

These functions are coordinated between two different user interfaces: the **Firewall Updates** page and the **Manage Firewalls** window.

> **Tip:** Before you begin to work with any updates, you should back up the current configuration of the firewall that is going to be updated. To perform this activity, click **Configuration Backup** in the **Firewall Maintenance** tree on the **Maintenance** icon.

The following procedure is a high-level overview of the way to perform these functions:

Steps

1) In the navigation bar, select **Maintenance**.

2) Click the **Firewall Updates** tab. The **Firewall Updates** page is displayed.

   > **Tip:** For option descriptions, press **F1**.

3) Select the firewall or firewalls to be updated in the **Firewall Updates** page.

4) Click **Manage Firewalls** to display the **Manage Firewalls** window.

5) On the **Packages** tab, select the action to be performed in the **Action** field. Different columns are displayed in the table, based on the value selected here.

   Rollbacks are available only if a previously installed update cannot be deleted. Also, consider the following information before you perform a rollback:

   - A rollback reverts the firewall to its state just prior to installation of the update package.
   - Changes that have been made to the firewall's configuration after the update package was installed will be lost.
   - A rollback is a recommended recovery option only for a short period of time after package installation.
   - A rollback always requires that the firewall is restarted.

   > **Tip:** For option descriptions, press **F1**.

6) Select the **Apply packages on all of the synced members** checkbox to keep the update versions in sync for all the cluster member nodes.

7) Select the updates to be installed, uninstalled, or rolled back.

8) [Optional] You can view a historical listing of all the update actions and status messages for this firewall on the **History** tab.

9) You can view the versions of software that are running on each cluster member node on the **Synced Members** tab.

10) When you have finished, click **Save**. The **Manage Firewall** window is closed and your selections are displayed on the **Firewall Updates** page.

11) Review your proposed changes. Then click **Update Firewalls**.

> **Note:** You cannot initiate a new update on a firewall while it has an update in the *In Progress* state.

12) You can monitor the status of the updates on this page in the **Update Status** column. You can also refresh the data on this page by clicking **Refresh Grid**.

Result

If the updates complete successfully, **Completed** should be displayed in the **Update Status** column.

Configuring software updates for a firewall

You can configure the software updates for all your firewalls on the **Manage Firewall** window.

If you are installing only one software update per firewall, you can perform that action on the **Firewall Updates** page. However, if you are installing more than one update per firewall or if you are uninstalling or rolling back updates, you must use the **Manage Firewall** window.

Additionally, you can view the update history of a particular firewall. You can also view the version of software that is installed on all the synced cluster members.

Related tasks
Install, uninstall, or roll back software updates on page 434

Schedule firewall updates

Use the **Schedule Firewalls** window to set a date and time for performing the following update actions on supported firewalls.

- Install
- Uninstall
- Rollback

You also can unschedule previously scheduled actions or perform these actions immediately.

Note: You can access this window only if you have selected at least one row in the table on the **Firewall Updates** page and each selected row must have an update selected for it.

Steps

1) In the navigation bar, select **Maintenance**.

2) Click the **Firewall Updates** tab. The **Firewall Updates** page is displayed.

3) Click **Schedule Firewalls** in the toolbar. The **Schedule Firewalls** window is displayed.

4) Schedule the date and time to perform an install, uninstall, or rollback on a firewall.

5) Click **Perform Actions Now** to perform the update actions immediately.

6) In **Devices and Actions**, specify types of actions to be performed on the firewalls.

7) Click **OK** to save these settings.

Configure update download settings

Use the **Update Settings** window to configure settings to download software updates for supported firewalls.

You can specify settings for the following features:

- Using a proxy server to download updates
- Using an auto-discovery process to identify and download available updates
- Displaying removed updates

Steps

1) In the navigation bar, click **Maintenance**.

2) Click the **Firewall Updates** tab. The **Firewall Updates** page is displayed.

3) Click the **Update Settings** tab. The **Update Settings** window is displayed.

4) In **Proxy Server Settings**, specify proxy server details to connect to a download site.

5) In **Auto-Discovery Settings**, specify the FTP or HTTP location available to your Management Server.

6) Click **Store Update Settings** to display removed updates on the **Stored Updates** page.

7) Click **OK**.

Storing firewall software updates

You can identify, store, and manage firewall software updates on the Control Center Management Server. Use the function that is available on the **Store Updates** page to perform these actions.

You can also manually download these updates to a specific location on the **Manual Download** window.

As updates become available for the firewalls that are configured in your environment, they can be downloaded from the FTP or HTTP auto-discovery location and stored on the Management Server. Use the **Store Updates** page to manage the download status and availability of the software updates.

There are two ways to identify when new updates are available:

- **Automatically** — Use the auto-discovery process when the Control Center Client is started. This feature is enabled by default on installation. However, it can also be configured in the **Update Settings** window.
- **Manually** — In the **Store Updates** page of the Control Center icon, click **Check For Updates**.

The **Store Updates** page displays all the identified updates for firewalls that have been previously defined in your configuration, along with the status of the update. The **Status** column displays the disposition of the update on the Management Server. You can:

- Determine whether the update is available on the Management Server.
- Download an update and store it on the Management Server.
- Check whether a download operation is still in progress or has failed.
- Check whether a previously downloaded update has been deleted from the Management Server.

If the status indicates that the update has not been downloaded, you can click **Download Updates** (from the toolbar) and store the update on the Management Server. The auto-discovery updates are downloaded from the FTP server to the Management Server by using parameters that are configured in the **Update Settings** window. You can also use the **Manual Download** window to download individual software updates manually to the Management Server from an alternate, user-defined location.

If an FTP or HTTP auto-discovery site is not available to your Management Server, an alternate location to use for the auto-discovery process can be created.

After the initial installation of the Control Center, the Control Center Client is automatically configured to use the auto-discovery process to check for new software updates each time that this application is started. You can also check for updates at any time by clicking Check For Updates (in the toolbar) on the **Store Updates** page.

Store software updates

Use the **Store Updates** page to identify, store, and manage firewall software updates on the Management Server.

Steps

1) In the navigation bar, select **Maintenance**.

2) Click the **Store Updates** tab. The **Store Updates** page is displayed.

3) Select a row. Details like name of the software update, firewall type, and date on which the update was released are displayed.

4) View status of an update to decide an action to perform.

5) Select an action to perform. You can check and download updates, restart downloading an update, or remove updates.

Manually download software updates

Use the **Manual Download** window to specify a location from which a specific update should be downloaded.

Steps

1) In the navigation bar, select **Maintenance**.

2) Click the **Store Updates** tab. The **Store Updates** page is displayed.

3) Locate the update to download and click **Manual Download** in the toolbar. The **Manual Download** window is displayed.

4) Specify the firewall type and protocol to download the software update.

5) Specify the file server from which the update is downloaded.

6) Specify the directory in which the update file is stored on the file server.

7) Select the file to be downloaded and provide your credentials.

8) Click **OK**.

Setting up an auto-discovery site

If the FTP auto-discovery site is not available to your Management Server and you want to configure an alternate location to use for the auto-discovery process, an auto-discovery file must be created. This file must be in a specific XML format.

The auto-discovery file is an XML file that describes the update packages. The following example displays the structure and content of an XML file for a firewall:

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CCAutoDiscovery>
 <packageSidewinder name="70000t01">
  <Description>Install new OPS kernels</Description>
  <FilePath>SW/70000t01</FilePath>
  <ReleaseDate>02/27/2007</ReleaseDate>
  <Time>1172608996</Time>
  <OS>Sidewinder</OS>
  <Revision>7.0</Revision>
  <Version>7.0.0.00</Version>
  <Type>E-Patch</Type>
  <Flags>active uninstallable</Flags>
  <Requires>70000</Requires>
  <Readme>Install new OPS kernels and reboot</Readme>
 </packageSidewinder>
 <packageSidewinder name="70000t02">
  <Description>Depends on 70000t01; installs new OPS kernels</Description>
  <FilePath>SW/70000t02</FilePath>
  <ReleaseDate>02/27/2007</ReleaseDate>
  <Time>1172609006</Time>
  <OS>Sidewinder</OS>
  <Revision>7.0</Revision>
  <Version>7.0.0.00</Version>
  <Type>E-Patch</Type>
  <Flags>inactive</Flags>
  <Requires>70000t01</Requires>
  <Readme>Depends on 70000t01; installs new kernel</Readme>
 </packageSidewinder>
 ...
</CCAutoDiscovery>
```

The tags that appear in the example file are described below:

- **<Description>** — Contains Information about the update package.
- **<File Path>** — Contains the relative path name of the update package.
- **<ReleaseDate>** — Contains the release date of the update package in MM/DD/YYYY format, where MM denotes the month, DD the day, and YYYY the year.
- **<Time>** — Contains the UNIX® operating system time stamp for the update package's build date.
- **<OS>** — Contains the name of the operating system for the firewall.
- **<Revision>** — Contains the release number for the main release (for example, 7.0).
- **<Version>** — Contains the firewall version to which the update package is applicable (for example, 7.0.1).
- **<Type>** — Contains the type of update package (for example, Patch, Hotfix, or E-Patch).
- **<Flags>** — Contains one of the following values that indicates the status: active, active uninstallable, inactive.
- **<Requires>** — Contains the names of other update packages on which this update package depends and that must be installed before this package or with this package.
- **<Readme>** — Contains the text for the readme file.
- **<Obsoletes>** — [Optional tag] Contains a wildcard value that is used to match the names of the packages that this update package will make obsolete.

PART VI

Control Center

Contents

Configure High Availability, administrators, roles and utilize the Support Tool on Control Center.

CHAPTER 34

Control Center icon overview

Contents

The **Control Center icon** provides configuration options for the Control Center Management Server.

About the Control Center icon

The following functions are available on the **Control Center** tree of the **Control Center** icon:

- **Settings** — Use the nodes beneath the **Settings** node on the **Control Center** tree to manage configuration of various settings of the Control Center Management Server.
  - **Network** — View and edit Control Center settings, such as host name, servers (NTP, DNS, and mail), network interfaces (IP address, net mask, broadcast, and gateway) and static routes on the **Network Settings** window.
  - **System** — Manage specific Control Center system settings in the **Control Center** icon. These settings include: specifying the default logon disclaimer information that is posted in the logon window for the Client application, the failed logon lockout settings, and the default application time-out period.
  - **Authentication** — Configure the way that Control Center users authenticate with the Management Server. The Control Center supports an internal authentication mechanism, as well as LDAP and RADIUS for off-box authentication.
  - **Date and Time** — Set the Management Server date and time in the **Date and Time** window.
  - **Server Properties** — Display and edit Control Center Management Server properties and add new properties.
  - **Firewall Audit Management** — Manage firewall audit log files that were written to the Control Center Management Server. You can export them to a remote location or you can delete them.
  - **Syslog** — Configure the syslog server or servers to which audit data from the Control Center will be sent.
  - **ePolicy Orchestrator** — Configure the Control Center Management Server to communicate with the ePolicy Orchestrator server to share information about host objects, firewalls, and the Control Center Management Server. To use this communication, you must also configure a McAfee ePO user in this window.
- **Maintenance** — Use the nodes beneath the **Maintenance** node in the **Control Center** tree to manage the backup and restoration of the Control Center configuration and the operational data. A full system backup can be requested and an off-box location can be specified.
- **Administrators** — Create Control Center administrators who can access the Control Center.
- **LDAP user groups** — Create and configure LDAP user groups who can access the Control Center.
- **Roles** — After a Control Center user (administrator) is specified, he or she is assigned a role that determines the tasks that he or she is allowed to perform. Although a default set of roles has been predefined, you can create additional administrator-defined roles that can be assigned to Control Center users.
- **Configuration domains** — Implement the configuration domains option to segregate configuration data views and management into multiple domains. The operation and configuration data associated with a configuration domain is accessible only when the specific domain is selected during the logon process. All

other configuration data is obscured and cannot be acted upon or seen. If configuration domains are activated, configuration domain versions and version management can be accessed from the **Control Center** icon.

- **Logs** — View and manage the settings to display log files from the Control Center Management Server. Additionally, you can view information about the Management Server.
- **Support Tool** — Create and save a configuration bundle file to assist technical support with troubleshooting.
- **High Availability (HA) configuration on the Management Server** — Use these wizards to establish or remove the High Availability (HA) Management Server configuration.

Also available in the Control Center icon are the following tabs:

- **MLC Connection Settings** — Displays the **MLC Connection Settings** page, in which you can view McAfee Logon Collector objects that contain configuration settings to communicate with the McAfee Logon Collector server.
- **Audit Trail** — Displays the **Audit Trail** page, in which you can list, filter, preview, and print the audit trail data. This page is read-only.
- **Alert Processing Rules** — Displays the **Alert Processing Rules** page in the work area, in which you can view all the alert processing rules that are currently available.
- **Control Center Updates** — Displays the **Control Center Updates** page, in which you can manage and install Forcepoint Sidewinder Control Center Management Server software updates.
- **Backup (Management) Server status** — If the High Availability (HA) Management Server Configuration option is used, you can view the status condition of the backup Management Servers in the **Backup Server Status** page.

CHAPTER 35

Control Center settings

Contents

Use the Control Center tree of the Control Center icon to manage Control Center Management Server settings.

About Control Center settings

You can manage several Control Center Management Server settings from the Control Center tree of the **Control Center icon**.

- **Network** — View and edit Control Center settings, such as host name, servers (NTP, DNS, and mail), network interfaces (IP address, net mask, broadcast, and gateway) and static routes on the **Network Settings** window.
- **System** — Manage specific Control Center system settings in the **Control Center icon**. These settings include: specifying the default logon disclaimer information that is posted in the logon window for the Client application, the failed logon lockout settings, and the default application time-out period.
- **Authentication** — Configure the way that Control Center users authenticate with the Management Server. The Control Center supports an internal authentication mechanism, as well as LDAP and RADIUS for off-box authentication.
- **Date and Time** — Set the Management Server date and time in the **Date and Time** window.
- **Server Properties** — Display and edit Control Center Management Server properties and add new properties.
- **Firewall Audit Management** — Manage firewall audit log files that were written to the Control Center Management Server. You can export them to a remote location or delete them.
- **SNMP Agent** — Configure the SNMP agent to use the SNMP get operation to query Control Center MIB-II tables.
- **Syslog** — Configure the syslog server or servers to which audit data from the Control Center will be sent.

- **ePolicy Orchestrator** — Configure the Control Center Management Server to communicate with the ePolicy Orchestrator server to share information about host objects, firewalls, and the Control Center Management Server. To use this communication, you must also configure a McAfee ePO user in this window.
- **FIPS** — Enable FIPS 140-2 processing on the Control Center.

Network settings

You can configure Control Center settings for your network by using the **Network Settings** window.

Configure Control Center network settings

Configure network settings from the **Network Settings** window.

Steps

1) In the navigation bar, select **Control Center**.

2) In the **Control Center** tree, expand the **Settings** node.

3) Double-click **Network**. The **Network Settings** window is displayed.

4) On the **General** tab, specify details like NTP, DNS, and mail configuration.

5) On the **Interfaces** tab, configure the interfaces for the node.

6) On the **Static Routes** tab, configure the static routes and enter details like default gateway, destination, and netmask for the static route.

7) Click **OK** to save the network settings.

System settings

You can configure the following system settings.

- Specify the disclaimer information that is displayed when users log on to the Control Center Client application.
- Specify the number of times that a user can unsuccessfully attempt to authenticate before being locked out.
- Specify the length of time that he or she is locked out if he or she failed to properly authenticate.
- Specify the default, system-wide, number of minutes that a user can be inactive, which means no keyboard activity or mouse movement, before he or she must re-authenticate to access the system.

Disclaimer information

One of the features of the Control Center is having the ability to place custom disclaimer information on the logon page of the Control Center Client application. You can use this information for any purpose.

For example, you can post general information of interest to other users on different shifts about general Control Center operations or configuration changes. The same information is displayed on the logon page of the Client application.

You can specify information directly on the **System Settings** window or you can browse for a previously created ASCII flat file to use.

> **CAUTION:** When you are writing the disclaimer information, if you press **Enter** for a line feed (advancement to the next line), the disclaimer will close. To insert line feeds, hold **Ctrl** and then press **Enter**.

Locking out users

To control firewall administration, most organizations tightly control the number of failed logon authentication attempts that are allowed before the user is temporarily locked out.

You can also control the length of time during which the user is prevented from authenticating. You can configure the default amount of time that a user can be idle (that is, with no mouse movement) before having to re-authenticate.

Each of these settings is managed in the **System Settings** window. Your system operators can impose the level of security that is appropriate for your organization.

Configure system settings

Configure system settings from the **System Settings** window.

Steps

1) In the navigation bar, select **Control Center**.

2) In the **Control Center** tree, expand the **Settings** node.

3) Double-click the **System** node. The **System Settings** window is displayed.

4) On the **Client Settings** tab, configure information for the Client application. You can timeouts, lockout details, disclaimer and security banner text, and set the security classification level.

5) On the **Change Tracking** tab, configure change tracking as implemented with the ticket and change report functions.

6) On the **Application Signature Updates** tab, configure the way that the Management Server will download updates to the application signature database.

7) On the **Dashboard** tab, configure the amount of time to store the resource data for Control Center. Configure settings for **Messages from Forcepoint** data and specify the frequency at which these files are downloaded and installed.

8) On the **Demo Mode** tab, enable or disable demo mode for the Client application.

9) Click **OK** to save the system settings.

Benefits of Control Center demo mode

Demo mode allows you to evaluate Control Center and experience the management console. In demo mode, Control Center demonstrates key features even if no real firewall exists.

- Ease of evaluation
- Test key features
- Create VMware images for distribution
- Capture demo data from a real firewall

In demo mode, you can view pre-populated objects, policies, dashboards, and reports.

Supported features

Demo mode supports these firewalls:

- High Availability
- SPAN firewall

Unsupported features

Demo mode does not support these features:

- Firewall on Crossbeam platform
- Real-time Audit
- Software upgrades for firewalls
- Firewall state changes like shutdown, restart, and halt
- Alerts

Enable and disable demo mode

You need to use the client application to turn on demo mode.

Before you begin

You must install a Control Center Management Server and Client application.

Steps

1) In the navigation bar, select **Control Center**.

2) In the **Control Center** tree, expand the **Settings** node.

3) Double-click **System**.

   The **System Settings** window is displayed.

4) In the **Demo Mode** tab, click **Turn on Demo mode**. Click **OK** for confirmation to restart the server.

   The Client application closes.

   Note: Click **Turn off Demo mode** to disable demo mode.

5) Log on to Control Center.

   The **User Name** and **Password** fields are pre-populated with the demo user credentials. The default demo user password is `ccadmin1`. The **Domain** shows **Demo**.

   Note: Once demo mode is disabled, these fields are blank. Enter your credentials. From the **Domain** drop-down menu, select the appropriate domain.

   Tip: We recommend you to change the password once you log in as a demo user.

6) Click **Connect**.

   Control Center is in demo mode.

Create and run virtual machine images

You can manually generate VMware images of the Control Center Management server. These files can be played on a VMware player, in turn creating a local instance of the virtual Control Center Management Server. However, you can set up a Control Center Management Server on a VMware server or workstation.

Before you begin

- Download and install VMware player.
- Extract and install the Virtual Network Editor (vmnetcfg.exe) to assign a subnet and name to the **Host-only** network.

A Control Center Client application can connect to the virtual Control Center Management Server and allow you to evaluate the key features.

Steps

1) Install Control Center server on a VM workstation.

   Refer to the *Forcepoint Sidewinder Control Center, Virtual Appliance Installation Guide* for details.

2) Select Network Adapter as **Host-only**.

3) Select **Edit** > **Virtual Network Editor** for the Host-only virtual subnet. Use the same management and gateway addresses for the Control Center server.

4) Log on to Control Center.

5) Go to **Control Center** > **Settings** > **System**.

   The **System Settings** window is displayed.

6) In the **Demo Mode** tab, click **Turn on Demo mode**.

7) After the server restarts, shut down the server using the `shutdown -h now` command.

   Virtual machine files (.vmx, .vmdk) are generated in the default folder `C:\Documents and Settings \Administrator\My Documents\My Virtual Machines.`

8) Select **Start** > **All Programs** > **VMware** > **VMware Player**.

   The VMware player window is displayed.

9) Click **Open**. Browse to the directory where the virtual machine files are stored. Select the .vmx file and click **Open**.

10) Log on to Control Center Client application. On the **Logon** window, click **Add or edit connection**.

    The **Add New Server** window is displayed.

11) Enter the server address and select the **Demo** checkbox.

    In the **Primary Server** area, the demo user credentials are populated.

12) Click **OK**. Click **Connect**.

    The Control Center Client application is connected to the virtual instance of the Control Center Management Server in demo mode.

Capture demo data from a real firewall

In demo mode, you can capture data from a real firewall and replace the existing static data. This data is called demo data.

Control Center uses pre-stored firewall configuration and reports in demo mode. When a firewall is added, this default configuration (static data) is used for retrieval and reports.

When you add a firewall, the newly captured data for that firewall is used for retrieval and reports.

Steps

1) In the navigation bar, select **Control Center**.

2) In the **Control Center** tree, expand the **Settings** node.

3) Double-click **Server Properties**. The **Server Properties window** is displayed. Configure these settings.
   - Deselect the **demo.isDemoMode** checkbox.

     ```
     demo.isDemoMode = false
     ```
   - Click **Add**. The **Add New Property** window is displayed.
     - Enter the property name as `demo.allowDemoDataCollection`. Select the checkbox.

       ```
       demo.allowDemoDataCollection = true
       ```
     - Select the property type as **Logical**.
     - Select the **Property value** checkbox.
     - Click **OK**.

4) Click **OK.**
   The server properties are configured.

5) Click **OK**.
   This restarts the server.

6) Log on to Control Center Client application and connect to the server.

7) Go to **Policy** > **Firewalls**. Add the firewall and only register the firewall.
   On the **Retrieve Firewall** window, click **Cancel** and don't retrieve the firewall.

8) When the firewall starts responding, expand the **Firewalls** node and select the firewall. Right-click the firewall and select **Collect Demo Data**.
   View the message at the start of data collection.

9) Check server logs for status of demo data collected.
   Collected data will be stored at default location `/use/local/tomcat/webapps/cm/WEB-INF/demoData/[Standalone|Cluster`. For example: `/use/local/tomcat/webapps/cm/WEB-INF/demoData/Standalone.`

Hard disk settings

The Control Center can be configured to shut down cryptographic operations if either the logs or database partition of the Management Server is full to prevent any loss of audit data. This is necessary for compliance with the Common Criteria standard.

Note: Shutting down cryptographic operations prevents remote access to the Control Center Management Server using SSH or from the Control Center Client application.

Configure Hard Disk settings for Common Criteria compliance

Configure the Control Center to shut down cryptographic operations when the partitions on the Management Server are full to prevent the loss of audit data. This is a requirement for Common Criteria compliance.

Note: Shutting down cryptographic operations prevents remote access to the Control Center Management Server using SSH or from the Control Center Client application.

Steps

1) In the navigation bar, select **Control Center**.

2) In the **Control Center** tree, expand the **Settings** node.

3) Double-click the **Hard Disk** node. The **Hard Disk Settings** window appears.

   Tip: For option descriptions, press **F1**.

4) Select the **Prevent loss of audit data** checkbox.

5) Click **OK**.
   All cryptographic operations will be shut down if either the logs or the database partition on the Management Server is full.

Authentication

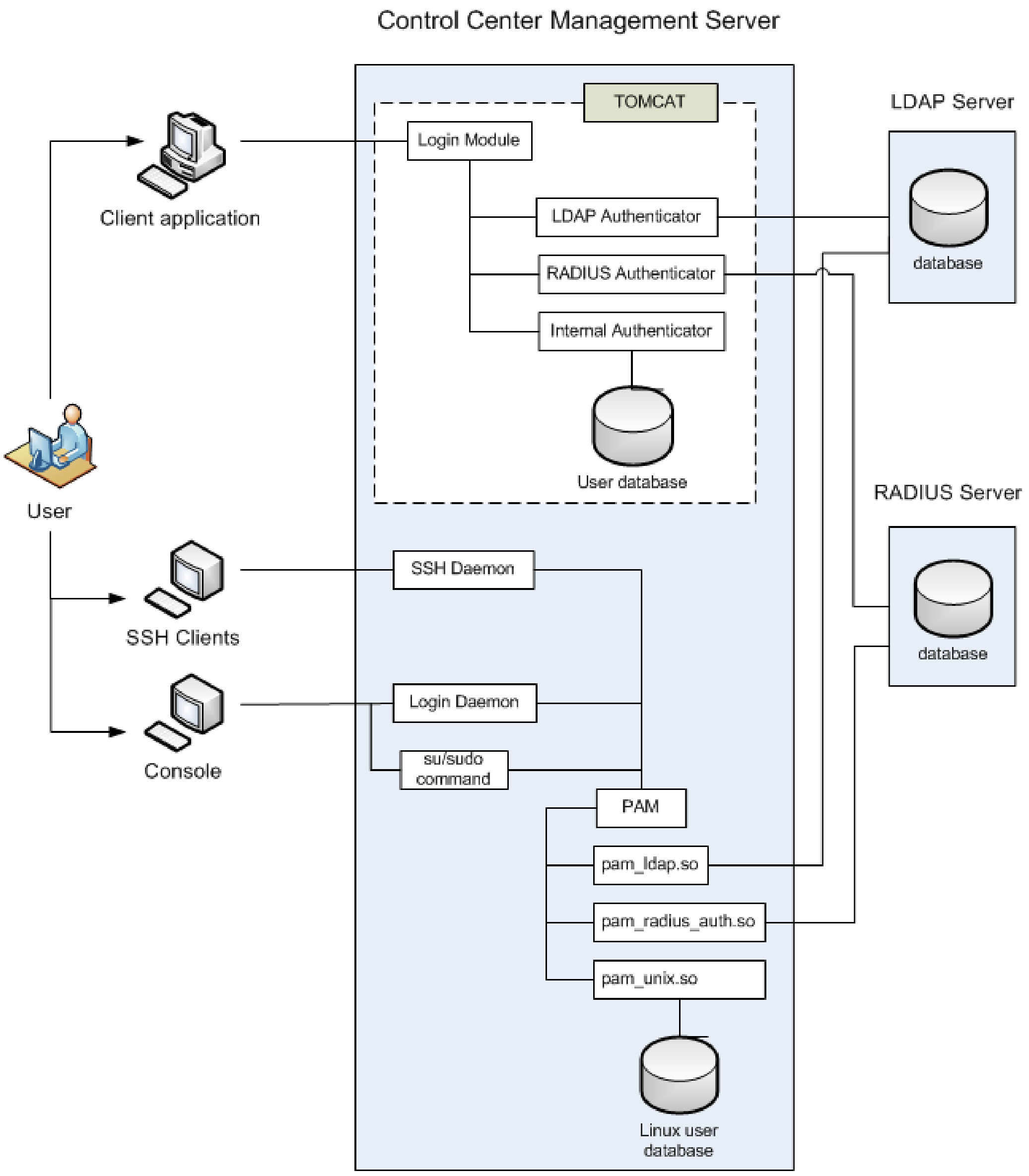
The Control Center supports using an external authentication mechanism, such as an LDAP or RADIUS server to provide off-box authentication support for Control Center users.

This feature currently supports the use of external servers to perform authentication. It does not support Control Center role-based, authorization management. This means that Control Center users and their associated passwords can be assigned and managed by using the mechanisms that are associated with the selected external servers. However, the Control Center internal authentication and authorization database must be updated and managed for each Control Center user to support the internal, role-based authorization mechanism.

Even if you have defined the authentication method as RADIUS or LDAP (in the **Authentication** window), SSH and console logons can still be authenticated by using internal authentication if the **Authenticate console and SSH logins using external authentication servers** checkbox is deselected (in that same **Authentication** window).

The following diagram displays the authenticator and server use for the different types of authentication.

Figure 27: Authentication for the Control Center user



User passwords

When you use external authentication, you can configure multiple external servers (LDAP or RADIUS) to manage the Control Center user passwords.

Each identified server is queried in the order that you specify (from top to bottom), as displayed in the **Authentication** window.

Use the **Authentication** window to select the authentication method. If either LDAP or RADIUS is selected, identify one or more external servers to use to authenticate Control Center users. You can use this window to configure additional server-specific configuration parameters for LDAP and RADIUS servers, as well as configurable port information.

To support the Control Center user role and configuration domain configurations, each Control Center user must be defined in the internal Control Center authentication database and any external LDAP or RADIUS server to support external authentication and internal user role authorization requirements. If you want to authenticate SSH and console logons by using external authentication servers, the user names of the `root` Linux accounts must be defined in the RADIUS or LDAP servers. If you want to upload firewall audit logs from the firewall to the Control Center Management Server, you must also define ftp Linux accounts in the RADIUS or LDAP servers.

Configuring LDAP authentication or RADIUS authentication

Standalone LDAP directory servers remove any need to deploy an OSI network. They can also be used directly over TCP/IP.

When RADIUS is used for user authentication, the credentials that were specified in the Control Center logon window are passed to a RADIUS server over the RADIUS protocol. For LDAP authentication only, you can also specify a distinguished name and password if you select the **Bind using specified credentials** checkbox. The RADIUS server checks that the information is correct. If the server accepts the information, it will then authorize access to the Control Center Management Server.

When you select **LDAP** or **RADIUS** as the value in the **Select authentication method field**, logons from the Client user interface are authenticated by using external authentication servers. The effect of this selection on console and SSH logons depends on the value of the **Authenticate console and SSH logins using external authentication servers** checkbox.

Authentication fallback

The Control Center authentication management scheme has an additional fallback feature.

If all the LDAP or RADIUS servers are unreachable and the user who is logging on to the Client has previously been designated for authentication fallback, the Control Center Management Server will authenticate the user by using the internal authentication database of the Management Server. You can enable this feature for any number of users by selecting the **Allow authentication fallback checkbox** on the Control Center **Administrator** window.

The user name synchronization requirement also applies to all Management Server users who must have their user name accounts specified in and synchronized with the external authentication servers. For Management Server user accounts, all defined Linux user accounts are automatically configured to have alternate internal authentication fallback.

If a Control Center user or Management Server Linux user account is forced to fall back to internal authentication, he or she will automatically switch back to external authentication the next time that he or she logs in to a Client application, a shell, or console account.

Use of the su and sudo commands

If you want to use the su or sudo commands at the Linux console of the Control Center Management Server or inside of an SSH session, you can be authenticated only against the internal password database of the Control Center Management Server.

These commands will not use external authentication.

Requirements for LDAP servers

Each Control Center administrator user should have a directory entry. The sAMAccountName attribute for each directory entry should contain the user name of the Control Center user.

Additional attributes can be available in the user's directory entry, depending on whether the Microsoft Windows Services for UNIX package is installed.

SSH logons

The LDAP server requirements also apply to the users who log on to the Control Center Management Server by using SSH.

- **Administrative user account** — Use this user account to connect to the Control Center Management Server by using SSH or the console logon.
- **Firewall Audit Export user account** — The firewall uses this user account to upload firewall audit logs by SCP, and to perform scheduled firewall configuration backups on the Control Center.

Console logons

The LDAP server requirements that are described above apply to users who log on to the Control Center Management Server by using the console of the Management Server.

Each user is listed, along with its role:

- **Administrative User account** — Management Server administrator
- **Database user account** — Database administrator

Configure Control Center user authentication

Access the **Authentication** window.

Steps

1) In the navigation bar, select **Control Center**.

2) In the **Control Center** tree, click the **Settings** node.

3) Double-click the **Authentication** node. The **Authentication** window is displayed.

4) On the **Authentication Servers** tab, specify the authentication servers. You can add, edit, or delete servers on this tab.

5) On the **Settings** tab, select the authentication method and configure authentication settings. You can select Internal, LDAP, or RADIUS authentication method.

6) Click **OK** to save these settings.

Configure external authentication servers

Access the Control Center **Authentication Server** window.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, expand **Settings** and double-click the **Authentication** node. The **Authentication** window is displayed.

3) Click the **Authentication Servers** tab.

4) Click **Add** or **Edit**. The Control Center **Authentication Server** window is displayed.

5) From the **Filter by Type** list, select the external authentication server you want to configure.

6) Click **Add**, **Edit**, or **Delete** to configure a server.

7) View the **Type** and **Port** details for the server.

8) Click **OK**.

Date and time

You can set the date and time on your Management Server from the **Date and Time** window.

Set the Management Server date and time

Configure the date and time from the **Date and Time** window.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, expand the **Settings** node.

3) Double-click the **Date and Time** node. The **Date and Time** window is displayed.

4) In the **Update Server Date and Time** options, specify the Management Server date and time.

5) Use the **Update Server Time Zone** fields to set the time zone.

6) Click **OK** to save these settings.

Server properties

To display and edit Control Center Management Server properties and to add new properties, use the **Server Properties** window.

Configure Management Server properties

Configure Management Server properties from the **Server Properties** window.

Steps

1) In the navigation bar, select **Control Center**.

2) In the **Control Center** tree, expand the **Settings** node.

3) Double-click the **Server Properties** node. The **Server Properties** window is displayed.

4) Click **Add** to define new properties.

   Note: After editing any existing value or introducing a new property, the Management server must be restarted for these changes to take effect.

5) Under **Property**, view the displayed properties and check for the new property.

6) Click **OK**.

system.statistics.collect.cron components

Refer to the following table for the components of the system.statistics.collect.cron property.

It consists of the following fields, separated by spaces. You can also use the asterisk (*) or wildcard character in any field and the question mark (?) character, which is an inclusive character, can be used in the **Day Of Month** and **Day Of Week** fields only.

Note: The system.statistics.cleanup.cron property has the cron property.

Table 39: Fields for the system.statistics.collect.cron property

Field number	Field name	Allowed values
1	Seconds	0–59
2	Minutes	0–59

Field number	Field name	Allowed values
3	Hours	0–23
4	Day Of Month	1–31
5	Month	1–12
6	Day Of Week	1–7
7	Year (optional)	empty or 1970–2099

Firewall audit log management

You can manage firewall audit log files that were written to the Control Center Management Server in the **Firewall Audit Management** window.

Although you configure the events that trigger the exportation in this window, the actual default exportation of this information occurs at 2:30 AM, Management Server time, unless you have edited the **`audit.export.cron`** property in the **Server Properties** Window. If you edit this property value, the exportation will occur at the time that you specify.

audit.export.cron components

Refer to the following table for the components of the **`audit.export.cron`** property.

It consists of the following fields, separated by spaces. You can also use the asterisk (*) or wildcard character in any field. The question mark (?) character, which is an inclusive character, can be used only in the **Day Of Month** and **Day Of Week** fields.

Table 40: Fields for the audit.export.cron property

Field number	Field name	Allowed values
1	Seconds	0–59
2	Minutes	0–59
3	Hours	0–23
4	Day Of Month	1–31
5	Month	1–12
6	Day Of Week	1–7
7	Year (optional)	empty or 1970–2099

For example, the following string indicates that the backup would occur at 2:30 AM every day of the week:

```
0 30 2 * * ? *
```

Manage firewall audit log files that are stored on the Control Center Management Server

You can manage firewall audit log files that were written to the Control Center Management Server in the **Firewall Audit Management** window.

You can specify two different areas that control the way that these files are managed:

- The criteria for export and deletion or only for deletion
- The action itself (export and then delete or only delete)

The way that you determine the targeted files for this is as follows:

- The files are more than *n* days old.

or

- The files are larger than a certain size that you specify.

In this scenario, when the size is exceeded, the files are deleted by starting with the oldest files first, until the amount of disk space is under the amount that you specified.

Export stored firewall audit log files to a remote location

You can export firewall audit log files that were written to the Control Center Management Server to a remote location.

After they are exported, they are deleted from the Control Center Management Server. Configure this process in the **Firewall Audit Management** window.

This is an ongoing activity that occurs each time that the Control Center Management Server processes firewall audit files. That time is scheduled in the **`audit.export.cron`** property in the **Server Properties** window.

Note: You cannot export files unless you also configure deletion.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, expand the **Settings** node.

3) Double-click the **Firewall Audit Management** node. The **Firewall Audit Management** window is displayed.

4) [Required] You must select one of the following deletion settings:

   - **Delete firewall audit files that are older than *n* days** — If selected, you must also specify the number of days to target for deletion.
   - **Limit the combined size of all of the audit files** — If selected, you must also specify the file size limit.

5) Configure the remaining fields in the Remote Location area.
   a) Select **Export firewall audit files from Control Center to a remote location prior to deletion**.

   > **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save these settings.

Delete stored firewall audit log files without exporting them

You can delete firewall audit log files that were written to the Control Center Management Server in the **Firewall Audit Management** window without having to export them to a remote server first.

This is an ongoing activity that occurs each time that the Control Center Management Server processes firewall audit files. That time is scheduled in the **audit.export.cron property** in the **Server Properties** window.

> **Note:** You do not have to export the files to be able to delete them. However, the reverse is not true. You can export the files only if you have configured deletion parameters.

Steps

1) In the navigation bar, select **Control Center**.

2) In the **Control Center** tree, expand the **Settings** node.

3) Double-click the **Firewall Audit Management** node. The **Firewall Audit Management** window is displayed.

4) [Required] You must select one of the following deletion settings:
   - **Delete firewall audit files that are older than n days** — If selected, you must also specify the number of days to target for deletion.
   - **Limit the combined size of all of the audit files** — If selected, you must also specify the file size limit.

5) [Optional] To export the files to a remote location before they are deleted, configure the remote location.
   a) Select **Export firewall audit files from Control Center to a remote location prior to deletion**.
   b) Configure the remaining fields in this area.

   > **Tip:** For option descriptions, press **F1**.

6) Click **OK** to save these settings.

Using the Control Center SNMP Agent

The Control Center SNMP Agent allows the Control Center Management Server to be monitored by network management stations using the SNMP (System Network Management Protocol) versions 1, 2c, and 3. You can configure the agent to use the SNMP get operation to query Control Center MIB-II tables and variables.

Use the Control Center Client application to configure the SNMP agent, and to configure SNMP communities and users. The Control Center SNMP Agent supports both SHA-1 and MD5 for authenticating SNMP connections, and DES and AES for privacy.

Log in as a root user. The Control Center-specific MIBs are available for download to an SNMP network management server at the following location:

```
/usr/local/etc/snmp/
```

Configure the Control Center SNMP Agent

You can configure the Control Center SNMP Agent.

Steps

1) Navigate to **Control Center** > **Settings** > **SNMP Agent**. The **SNMP Agent** window appears.

   Tip: For option descriptions, press **F1**.

2) Select **Start SNMP Daemon**.

3) Enter location and contact information.

4) Select the versions of the SNMP protocol you want to allow.

5) If you are allowing SNMP version 1 or 2c, add the get communities you want to allow.

6) If you are allowing SNMP version 3, add the users you want to allow.

7) Click **OK**. Your configuration changes are saved, and the window closes.

Result

The SNMP Agent starts transmitting Control Center Management Server information to the network management system.

ePolicy Orchestrator settings

The McAfee® ePolicy Orchestrator® (McAfee ePO™) platform provides a scalable platform for centralized policy management and enforcement of your security products and the systems on which they reside.

It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

The Control Center and the ePolicy Orchestrator can share data about host objects and firewalls. The Control Center can display information that it has obtained from the McAfee ePO server about hosts that are referenced in a policy or hosts that are passing traffic through the firewall. The ePolicy Orchestrator can display health and status information about firewalls and the Control Center Management Server that it has obtained from the Control Center.

To be able to view the data on either the Control Center or on McAfee ePO, you must install the ePolicy Orchestrator Extension for Sidewinder on the McAfee ePO server. For more information about this, see *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide* 5.3.2.

To be able to view data from the ePolicy Orchestrator server about hosts on the firewalls, the following prerequisites must be met:

- The ePolicy Orchestrator Extension for Sidewinder must be installed on the McAfee ePO server that you will configure in the **ePolicy Orchestrator Settings** window.
- You must configure settings for the McAfee ePO server in the **ePolicy Orchestrator Settings** window. This is to allow the Control Center to communicate with the McAfee ePO server. For the McAfee ePO server to communicate with the Control Center, a McAfee ePO user must also be defined on the Control Center.
- On this same window, you must have selected the **Allow Control Center to retrieve reports from the ePO server** checkbox.

After these prerequisites have been met, you can view ePolicy Orchestrator data for individual hosts from the host object in the **Policy** tab (by right-clicking a host object and selecting **Show ePO Data**) or from the **Firewall Audit** page (by right-clicking the **Source IP** or the **Destination IP** row value on the page and selecting **Show ePO Data**).

Configure access to the ePolicy Orchestrator server

Configure ePolicy Orchestrator server access from the **ePolicy Orchestrator Settings** window.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, click the **Settings** node.

3) Double-click the **ePolicy Orchestrator Settings** node. The **ePolicy Orchestrator Settings** window is displayed.

4) On the **Control Center User** tab, create and edit the ePO user object. You can create only one user with the ePolicy Orchestrator role.

5) Click **Edit** or **Delete** to modify or delete an existing user.

6) Click **OK**.

View ePolicy Orchestrator host data

To view ePO host data, access the **ePO Host Data** page.

Steps

1) In the navigation bar, select **Policy**.
2) Click the **Rule Objects** tab.
3) Expand the **Network Objects** node.
4) Select the **Hosts** subnode. All the defined host objects are displayed.
5) Right-click the object for which you want to view McAfee ePO data and select **Show ePO Data**. The **ePO Host Data** page is displayed.

   Note: This option is available only if you have selected the **Allow Control Center to retrieve reports from the ePO server** checkbox on the **ePolicy Orchestrator Settings** window. You can also access this report by generating the audit report and from the **Firewall Audit** page, right-clicking the **Source IP** value or the **Dest IP** value in any row and selecting **Show ePO Data**.

6) View data for the selected host object. You can see details like host name, name, and value for the host parameter.

Using ePolicy Orchestrator to monitor firewalls

You can use Control Center to configure managed firewalls so that firewall details can be viewed in ePolicy Orchestrator dashboards.

ePolicy Orchestrator uses firewall data to more accurately assess the risk levels of the traffic flowing through your network. With insight into the risk-level of the traffic on your network, you can tailor your policy to limit or eliminate traffic that might be carrying viruses, spyware, or malware.

See the *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide*, version 5.3.2 for instructions on installing and configuring the extension.

Configure managed firewalls for ePolicy Orchestrator reporting

Use the Control Center Client application to set up a managed firewall to pass information to ePolicy Orchestrator.

Note: Only firewalls at version 8.2.1 and later can be configured to send information directly to ePolicy Orchestrator.

Steps

1) Create an ePolicy Orchestrator settings object.
   a) From the Control Center Client application, click **Policy**.
      The Policy icon page appears.
   b) On the Firewall Settings tab, right-click **ePolicy Orchestrator** , then select **Add Object**.
      The ePolicy Orchestrator window appears.
   c) Enter a name and description for theePolicy Orchestrator settings object.
   d) Select **Enabled**.
   e) Enter the IP address of the ePolicy Orchestrator server.
   f) Enter the user name and password used to communicate with the ePolicy Orchestrator server.
   g) Click **Retrieve ePO root certificate**. The ePolicy Orchestrator root certificate is added to and selected in the CA certificate list.
   h) Click **OK**.

   The new ePolicy Orchestrator settings object appears on the Firewall Settings tab under the ePolicy Orchestrator node.

2) Apply the ePolicy Orchestrator settings object to a managed firewall.
   a) In the Policy area, double-click the firewall.
      The Firewall window appears.
   b) Click **Offbox**.
      The Offbox area appears.
   c) In the ePolicy Orchestrator section, from the Configuration drop-down list, select the ePolicy Orchestrator settings object you created in step 1.
   d) Click **OK**.
      The Firewall window closes.
   e) Click **Apply**.
      The Apply Configuration window appears.
   f) Select the firewall, then click **OK**.
      The ePolicy Orchestrator settings are applied to the firewall.

Result

The firewall sends information to the ePolicy Orchestrator server. Firewall details can be viewed on ePolicy Orchestrator dashboards.

Control Center and FIPS

For more information on configuring Control Center for FIPS 140-2 compliance, see the *Firewall Enterprise Control Center FIPS 140-2 Configuration Guide*.

Controlled access with SELinux

Security-Enhanced Linux (SELinux) in Control Center enables you to support access control security policies. This acts as another layer of security and hardens the Control Center system.

By default, when you install Control Center 5.3.2 Patch 2 or upgrade from earlier versions to 5.3.2 Patch 2, SELinux is enabled. As a root user, you can modify and check the SELinux settings.

Important: You can't disable SELinux on Control Center.

SELinux can be either in `permissive` or `enforcing` mode. The default `enforcing` mode enables and enforces SELinux policies to restrict access and log actions. The `permissive` mode enables SELinux, but does not enforce the security policy. It only allows to warn and log actions.

Check SELinux status

You can check if SELinux is enabled on Control Center and view the policy and mode. Log on as a root user and execute:

```
-bash-4.1# sestatus
```

The output is as shown.

```
SELinux status: enabled

SELinuxfs mount: /selinux

Current mode: enforcing

Mode from config file: enforcing

Policy version: 26

Policy from config file: targeted
```

Change modes

You can either modify the SELinux modes on a temporary basis or permanently.

To temporarily change from `enforcing` to `permissive` mode:

1) As a root user, check the current SELinux mode: `-bash-4.1# getenforce`. The current mode is `enforcing`.

   Tip: In FIPS mode, Control Center does not allow to login as root user. Use `sudo sestatus` to check the SELinux status.

2) Execute the command: `-bash-4.1# setenforce 0`

3) Verify the mode is changed: Execute`-bash-4.1# getenforce`. The mode is changed to `permissive`.

To permanently change from `enforcing` to `permissive` mode:

1) As a root user, navigate to /etc/selinux/config and change `SELinux=permissive`.

2) Reboot the system.

3) Verify the SELinux status: Execute `-bash-4.1# sestatus`.

⚠ **Important:** If Control Center is in FIPS mode, permanently changing the SELinux mode is not supported. If you wish to permanently change the mode, change it prior to enabling FIPS mode.

CHAPTER 36

Control Center maintenance

Contents

The Management Server contains all the configuration information for one or more security policies that have been implemented for the enterprise, or, as in the case where configuration domains have been configured, multiple enterprise class domains.

The data that is stored on the Management Server is critical to the management of the firewalls and their implemented security policies. Establishing a security practice to make sure the ability to restore this critical data in case of catastrophic failure is fundamental to the operation of the enterprise.

Backing up configuration data for the Management Server

You can back up your data in three different ways.

- Backing up automatically every night
- Backing up the Management Server by using the user interface
- Backing up the Management Server files by using the command line

The following table provides information about the types of files that are backed up by each of these methods.

Table 41: Backed up files by backup method

Type of files	Automatic nightly backup	User Interface (Backup Control Center System window with Full system backup checkbox selected)	User Interface (Backup Control Center System window with Full system backup checkbox deselected)	backuptool command
Configuration database (cg_configuration)	Yes	Yes	Yes	Yes
System database (cg_system)	Yes	Yes	No	Yes
Events database (cg_events)	Yes	Yes	No	Yes

Type of files	Automatic nightly backup	User Interface (Backup Control Center System window with Full system backup checkbox selected)	User Interface (Backup Control Center System window with Full system backup checkbox deselected)	backuptool command
CA and SSL certificates and private keys	No	Yes	No	Yes
Firewall and Control Center Management Server software updates	No	Yes	No	Yes
Secure Alerts Server configuration files and miscellaneous other files	No	Yes	No	Yes
Firewall audit log files and configuration backups	No	Yes if the checkbox for the **backups.auditlogs** setting is selected in the **Server Properties** window	No	Yes, unless the `-L` option is specified
Backup files contained in `/var/cc/backups/server/cfgbackups` and `/var/cc/backups/server/nightlybackups` This includes the nightly backups and the backups that were created by using the user interface.	No	Yes if the checkbox for the **backups.dbbackups** setting is selected in the **Server Properties** window	No	Yes, unless the `-D` option is specified
Backup files contained in the `/var/cc/backups/server/cfgbackups`. A scheduled job runs at 1.45 a.m. local time everyday to maintain the backups. The most recent full system backup is never deleted. **Note:** If the number of old backups is less than the value set for **backup.generations**, none of the old backups are deleted.	No	Yes if the value for **backup.generations** is set to default value of -1 in the **Server Properties** window, all the backups are retained. This value specifies the number of backups retained in the system. For example, if this value is set to 4, only four recent backups based on the timestamp are retained and the rest are deleted.	No	Yes

Backing up automatically every night

By default, backup files of the configuration (cg_configuration), system (cg_system), and events (cg_events) database data occur at midnight each night.

Note: These files are stored locally on the Management Server. It is recommended that you also back up these files to an off-box location.

- **cg_system** — This database includes information about the Control Center system, software update data, backup information, deployment information, and similar data.
- **cg_configuration** — This database includes all the firewall configuration data, configurable objects data, certificates, and similar data.
- **cg_events** — This database includes all the information that the Monitor icon extracts from the syslog files that are used to monitor firewall activity and to generate various reports.

Seven revisions of this data are stored in the `/var/cc/backups/server/nightlybackups` directory. Each revision is identified by a date and a numeric identifier. The `root user` Linux account has the necessary privileges to modify the characteristics of this cron job, as required, and to restore individual configuration, system, and events database data.

Backing up the Management Server by using the user interface

You can perform backups of your Management Server by using the **Backup Control Center System** window.

By using this window, you can perform the following tasks:

- Save your configuration files immediately (either locally or off-box)
- Create a schedule on which to save your configuration files (either locally or off-box)

If configuration domains are active, you can access the **Backup System** and **Restore System** menu options from the **Maintenance** node in the **Control Center** tree of the **Control Center** icon.

Back up your configuration files

Use this procedure to create a backup of your Control Center configuration.

Steps

1) Navigate to the Backup Control Center System window.
    a) In the navigation bar, select **Control Center**.
    b) In the Control Center tree, expand **Maintenance**.
    c) Double-click the **Backup System** node. The Backup Control Center System window is displayed.

2) Configure the fields in this window, depending on whether you are saving the configuration locally or sending it off-box and whether you are scheduling the backup or performing it immediately. If you save the configuration files locally, they are saved into the following directory:

   /var/cc/backups/server/cfgbackups

3) To create a full system backup, make sure that the **Full system backup** checkbox is selected. If you do not select this checkbox, only the cg_configuration database will be included in this backup file. The full system backup file includes all the firewall configuration data, configurable objects, certificates, and similar data. Note that database backups and audit log backups will not be included in the default full system backup. To add these into your full system backup, you must configure the following settings on the Server Properties window:

   ```
   backup.auditlogs
   ```

   ```
   backup.dbbackups
   ```

   Note that the inclusion of these backups will greatly increase the size of your backup files.

4) Click **Add** to save your configuration information. Click **Close**.

Backing up the Management Server files by using the command line

As the `Administrative` user, you can manage the configuration, system, and events database data by using the `backuptool` command. To back up databases only, use the `backupdb` command.

Backuptool command overview

Use the `backuptool` command to back up or restore full backups of your Management Server configuration.

Access the backuptool command in the /usr/sbin/ directory by using the sudo command as follows:

```
sudo /usr/sbin/backuptool <options>
```

Run this command without arguments to view all the available options. The following commands are examples of the backup command of the backuptool and all the available parameters.

It is important that you review these procedures because there are some important prerequisites that are included in them.

```
sudo /usr/sbin/backuptool
backuptool backup -f filename[.des3] [-k passphrase] [-L] [-D]
backuptool restore  -f filename[.des3] [-k passphrase] [-a adminpassword]
[-L] [-D] [-b] [-i]
backuptool extract  -f filename
backuptool download -f filename -s scheme -h hostname -d \remote-directory -u username -p password
backuptool upload   -f filename -s scheme -h hostname -d \remote-directory -u username -p password
```

where:

`[.des3]`	Optionally use to encrypt file during backup and decrypt during restore
`[-k]`	Encryption passphrase is the next argument in the command. The file name must have a .des3 extension.

`[-L]`	Excludes files in `/var/cc/audit` from the backup or restore operation
`[-D]`	Excludes files in `/var/cc/backups/server/backups` and in `/var/cc/backups/server/nightlybackups` from the backup or restore operation
`[-a]`	Password of an Admin user, for example, mgradmin
`[-b]`	Treats the backup file as having been created on a CC HA system
`[-i]`	Ignore the release level of the backup file
`filename`	file name of archive file
`passphrase`	encryption passphrase
`adminpassword`	admin user password used only while restoring a High Availability pair
`scheme`	one of FTP,FTPS,SCP
`host`	host name [:port(optional)] (When using FTPS, port is either 21 or 990. Consult your FTP server documentation.)
`remote-directory`	directory on remote host
`username`	username on remote host
`password`	password on remote host

The lines prefixed by `%GCC` indicate the result of the backuptool command. Here, the output indicates a problem with the arguments that were passed. Therefore, the command prints use information, as well as the summarized result.

`%GCC: REASON`	The first argument passed to backuptool was incorrect.
`%GCC: STATUS`	ERROR
`%GCC: CODE`	1

If the backuptool command fails, it returns `STATUS=ERROR and CODE=<a non-zero error code>`. It might optionally return a `REASON=<the cause of the error>`.

The `-k` option requires a passphrase argument and the file name must have a .des3 extension. The passphrase that you provide will be used to encrypt backup files for backup operations and decrypt backup files for restore operations. The restore will fail if the passphrase that is used for restoring backups does not match the passphrase that was used to create the backup.

Tip: When you specify a passphrase from the command line, shell quoting rules apply.

The following command is an example of the command to create a backup file by using hello'world as the passphrase:

```
sudo /usr/sbin/backuptool backup -f test.bak.des3 -k "hello"\''world'
```

The `-L` option omits the audit log files. Audit log files can get very large and can significantly increase the amount of time that it takes to back up or restore the system. If you do not back up audit log files, historical information that is used in reporting functions for all managed firewalls when a Management Server is restored from a backup is eliminated.

The `-a` option must be specified only when the system is set in High Availability mode.

The `-D` option omits the backup files in the `/var/cc/backups/server/cfgbackups` and `/var/cc/backups/server/nightlybackups` directories. The current database configuration is preserved. However, the daily backup files that are automatically created each night (a total of seven files) and the user-created backup files that are created by using the user interface are not included in the backup. If you include these files in the backup, the amount of time it takes to backup or restore the system can significantly increase. If you do not back up these database backup files, you lose the ability to restore them when a Management Server is restored from a backup.

The `-f` option requires a path argument. The path identifies the complete path and file name of the archive file that is being created or restored. The file name must be identical to the name of the file on the remote host. (The directory part does not need to match.)

If the path argument for the `-f` option ends in `.des3`, the backup file will be encrypted or decrypted, respectively, for the backup and restore operations.

The `-i` option ignores the release version of the backup file. The backup file will be restored, even if it was created while running a different release of the Management Server. This is not usually recommended.

The `hostname` argument that is supplied with the `-h` option must be able to be resolved by the Management Server, or the administrator can alternately specify an IP address. An optional port value can be specified if it is required by the host.

Related tasks

Create backup files for all databases on page 472

Create backup files for a single database on page 472

Create a backup file for a full system restoration on page 473

Create backup files for all databases

Back up all the database files.

Before you begin

Make sure that no users are accessing any of the databases.

Steps

1) Log on to the Management Server. Database backup files are written to the current directory. Make sure that the current directory is the one that will be written to by the `Administrative` user (for example: `/home/<Administrative user>`).

2) Run the following command:

```
sudo /usr/sbin/backupdb all
```

Backup files are created for each of the three databases in the current working directory.

Create backup files for a single database

Back up any one of the database files.

Steps

1) Make sure that no other users are accessing the database.

2) Log on as the `Administrative` user. Database backup files are written to the current directory. Make sure that the current directory is the one that will be written to by the `Administrative` user (for example, `/home/<Administrative user>`).

3) Run the following command:

   `sudo /usr/sbin/backupdb [-k` *`passphrase`*`]` *`database-name backup-file`*`[.des3]`

   where *`database-name`* is `cg_system` for the system database, `cg_configuration` is the name for the configuration database, or `cg_events` is the name for the events database data collected by the Secure Alerts server. To create an encrypted backup file, append the optional `.des3` file extension to the backup file name. You can specify a customized encryption passphrase for encrypted backup files by using the optional `-k` parameter. Note that standard shell quoting rules apply.

   For example, `sudo /usr/sbin/backupdb -k 'secret' cg_events cg_events.bak.des3`

Create a backup file for a full system restoration

You should designate a specially named directory on the remote FTP server to store the backup so that it can be easily located during the restore process.

You can view the progression of a backup on the **Restore System from Backup** window.

Use the following procedure to create a full system backup that will include:

- Backup files in the `/var/cc/backups/server/cfgbackups` and `/var/cc/backups/server/nightlybackups` directories
- Firewall audit log files

Steps

1) Log on as the `Administrative` user.

2) Make sure that the backup user has access to the current directory (for example, `/tmp`). Database backup files are written to the current directory.

3) As `Administrative` user, create the backup file:

```
sudo /usr/sbin/backuptool backup -f filename[.des3] [-k passphrase]
```

   where:

`filename`	file name of archive file
`[.des3]`	Optionally use to encrypt file during backup and decrypt during restore.
`[-k` *`passphrase`*`]`	Optionally encrypt the file by using a custom encryption passphrase. The file name must use the.des3 extension. A default passphrase will be used if no passphrase is specified.

4) Move this backup file to a safe, off-box location by using the following command-line command as `Administrative` user:

```
sudo /usr/sbin/backuptool upload -f filename -s scheme -h hostname -d remote-directory -
u username -p password
```

where:

filename	file name of archive file
scheme	one of FTP, FTPS, SCP
host	host name [:port(optional)] (When using FTPS, port is either 21 or 990. Consult your FTP server documentation.)
username	username on remote host
password	password on remote host

Restoring configuration data to the Management Server

You can restore configuration data to a Management Server by using the user interface (the **Restore System from Backup** window), or by using the command-line interface.

If you want to restore configuration backup files from Management Servers in a High Availability configuration, you should use the command-line tools. You can take a backup from the High Availability pair and restore the pair without having to break the pair.

On a standalone Control Center system, when you perform a backup and restore, the system restores automatically. However, for a High Availability pair, you need to enter the login password to restore the High Availability pair successfully. You can restore using the command-line tools or from the Control Center client.

Note: While restoring the backup on an HA pair, use the same user credentials on which the HA backup was initially taken.

Related tasks

Restoring Management Servers that have failed completely on page 478

Restore configuration data using the user interface

Use the **Restore System from Backup** window to restore a user-defined configuration file that is stored locally or off-box, or to restore a system-generated configuration file that was automatically generated before a retrieve was performed.

The *system-generated* backups that are displayed on this window contain the cg_configuration database data only, which includes all the firewall configuration data, configurable objects data, certificates, and similar data.

Steps

1) In the navigation bar, select **Control Center**. In the **Control Center** tree, click **Maintenance**. Then double-click the **Restore System** node. The **Restore System from Backup** window is displayed.

2) Select the backup file to use and click **Restore**.

   Note: If the backup file is located on a remote server, the **Remote Username and Password** window is displayed.

   Note: If the backup file to restore is stored on the Client system, you can upload the file to the Management Server by clicking **Upload** and then follow the instructions on the window. After the file has been uploaded, the backup file should be displayed in the list of available backups. For a restore in HA, select **Backup was created on a high availability system** and follow the instructions.

   Tip: For a standalone setup, the system comes up automatically. For an HA pair, during restoration enter the password at the prompt. This restores a standalone system and HA pair successfully.

3) Click **Restore** and **Yes** on the confirmation dialog box. The following results can occur:

   - **Successful restore of full backup** — You will be logged off of the Client application and the Management Server will be restarted. You will not be allowed to log back in until the restore has finished.
   - **Successful restore of configuration backup** — A message is displayed, indicating that the restoration was successful and advising you to log off and to restart the Management Server. Click **OK** and take the recommended actions—log off, restart the Management Server, and then log on again.
   - **Failed to restore** — If the errors cannot be resolved, contact technical support for additional assistance.

Restore data using the command line

The following procedures address restoration of various components of configuration data by using the command line interface.

Related concepts

Backuptool command overview on page 470

Restore all the databases for a Management Server

Restore all Control Center databases.

Steps

1) Make sure that no other users are accessing the database.

2) Log on as the `Administrative` user.

3) Stop all user interface clients, Tomcat, and Secure Alerts because open database connections will interfere with the restore process.

   To stop Tomcat:

```
su root
/etc/init.d/tomcat stop
```

   To stop Secure Alerts:

```
su root
/etc/init.d/dcserver stop
```

4) Change the directory to the location where the backup files are located. Make sure that the current directory contains all the databases that were previously saved by using the `/usr/sbin/backupdb all` command. When you have configured the HA Management Server feature, you must remove this function before you restore any data.

5) Run the following command:

```
/usr/sbin/restoredb [-d] [-b] all
```

   The optional `[-d]` parameter is used primarily by technical support. Use this parameter only if instructed to do so by technical support. The `[-b]` parameter must be specified when the backup being restored was created while the HA feature was operational.

   Note: During this `restoredb` session, you will be prompted to specify the password for the `root` user account several times. You must provide it for the restoration to continue.

6) After successfully restoring the backup file, start Tomcat and the Secure Alerts server.

   To start Tomcat:

```
/etc/init.d/tomcat start
```

   To start the Secure Alerts server:

```
/etc/init.d/dcserver start
```

Related tasks

Remove Management Servers from HA configuration on page 518

Restore a single database

Restore a Control Center database.

Steps

1) Make sure that no other users are currently accessing the database.

2) Log on as the `Administrative` user.

3) Stop all user interface clients, Tomcat, and Secure Alerts because open database connections will interfere with the restore process.

   To stop Tomcat:

   ```
   sudo /etc/init.d/tomcat stop
   ```

   To stop Secure Alerts:

   ```
   sudo /etc/init.d/dcserver stop
   ```

   To switch to the `root` user, run the following command:

   ```
   su root
   ```

4) Change directories to the location where the backup is located (for example: `/home/root`). If you are restoring a database file from the nightly backups, change the current directory to the nightly backup directory (`/var/cc/backups/server/nightlybackups`). When you have configured the HA Management Server feature, you must remove this function before you restore any data.

5) Run the following command:

   ```
   /usr/sbin/restoredb [-d] [-b] [-k passphrase] database-name backup-file[.des3]
   ```

   where *`database-name`* is `cg_system` for the system database, `cg_configuration` is the name for the configuration database, or `cg_events` is the name for the events database data that is collected by the Secure Alerts server. The optional `[-d]` parameter is used primarily by technical support. Use this parameter only if instructed to do so by technical support. The `[-b]` parameter must be specified when the backup being restored was created while the HA feature was operational. The optional `.des3` file extension indicates that the file will be automatically decrypted. Use the optional `[-k]` parameter to decrypt the backup file with a custom encryption passphrase if a custom passphrase was specified when the backup file was created.

   The following example restores an encrypted `cg_events` database file to the `cg_events` database on the current Management Server:

   ```
   /usr/sbin/restoredb cg_events cg_events.bak.des3
   ```

   Note: During this `restoredb` session, you will be prompted to specify the password for the `root` user account several times. You must provide it for the restoration to continue.

   This next example restores a `cg_configuration` database file that was encrypted with a custom passphrase:

   ```
   /usr/sbin/restoredb -k 'secret' cg_configuration cg_configuration.bak.des3
   ```

6) After successfully restoring the backup file, you should start Tomcat and the Secure Alerts server:

   To start Tomcat:

   ```
   /etc/init.d/tomcat start
   ```

   To start the Secure Alerts server:

   ```
   /etc/init.d/dcserver start
   ```

Restore the Management Server configuration files from the command line

Use the `Administrative` user account to access the `backuptool restore` command in the `/usr/sbin/` directory by using the `sudo` command.

The following command is an example of the restore command of the backuptool and all the available parameters.

It is important that you review these procedures because there are some important prerequisites:

```
sudo /usr/sbin/backuptool restore -f filename[.des3] [-k passphrase] [-a
adminpassword][-L]\[-D] [-b] [-i]
```

where:

filename	File name of archive file
`[.des3]`	Optionally use to encrypt file during backup and decrypt during restore.
`[-k passphrase]`	Optionally use the specified passphrase to encrypt the backup file.
`[-a adminpassword]`	password of an Admin user, for example, mgradmin. This must be specified only when restoring in High Availability mode.
`[-L]`	Do not include audit log files.
`[-D]`	Do not include database files.
`[-b]`	This argument must be specified if file was created when CC HA was active.
`[-i]`	Ignore the release level of the backup file.

Related tasks

Restore all the databases for a Management Server on page 475

Restore a single database on page 476

Restoring Management Servers that have failed completely

If you have a standalone Management Server or one or both servers in a High Availability (HA) configuration that fail completely, the following topics provide procedural information for restoring the Management Server (or Servers).

Make a note of these points for an HA pair:

Steps

- Disable external authentication like LDAP or RADIUS, take a CCHA backup, and then allow the HA pair to be restored.
- While restoring an HA pair, you will be required to enter a password.
- When you restore a High Availability pair, backup from primary must be restored on primary server and backup from secondary must be restored on secondary server.

Restore a standalone Management Server that has failed completely

If a Management Server experiences a total system failure and it must be recovered from a backup, perform the following steps.

Steps

1) Perform a complete installation of the Management Server on the new server by using the installation USB drive that was included with the Control Center. Follow the installation instructions.

2) Log on to the Management Server console as the `Administrative` user.

3) Make sure that the backup user has access to the current directory (for example, /tmp). Then run the `backuptool` command as listed below to move the backup file to be restored into the current directory location.

```
sudo /usr/sbin/backuptool download -f filename -s scheme -h hostname -d remote-directory -
u username -p password
```

where:

filename	path and file name of archive file
scheme	one of FTP, FTPS, SCP
hostname	host name [:port (optional)] (When using FTPS, port is either 21 or 990. Consult your FTP server documentation.)
remote-directory	directory on remote host
username	username on remote host
password	password on remote host

4) Stop all Control Center Client applications, Tomcat, and Secure Alerts because open database connections will interfere with the restore process.

To stop Tomcat:

```
sudo /etc/init.d/tomcat stop
```

To stop Secure Alerts:

```
sudo /etc/init.d/dcserver stop
```

5) The backup file can now be restored.

   When the backup is restored, the backuptool will check to make sure that the release level of the backup file matches the release that is currently running on the Management Server. If the release levels do not match, the backup will not be restored.

   If the backup file was created by using the command line process, any components that were excluded from the backup (such as database backups or audit log files) should be indicated during the restore process by using the [-L] and [-D] parameters.

   As Administrative user, issue the command line restore command:

```
sudo /usr/sbin/backuptool restore -f filename[.des3] [-k passphrase] [-L][-D] [-b] [-i]
```

   where:

filename	file name of archive file
[.des3]	Optionally use to encrypt file during backup and decrypt during restore.
[-k *passphrase*]	Optionally use the specified passphrase to encrypt the backup file.
[-L]	Do not include audit log files.
[-D]	Do not include database files.
[-b]	This argument must be specified if file was created when CC HA was active.
[-i]	Ignore the release level of the backup file.

6) After successfully restoring the backup file, you should start Tomcat and the Secure Alerts server:

   To start Tomcat:

```
sudo /etc/init.d/tomcat start
```

   To start the Secure Alerts server:

```
sudo /etc/init.d/dcserver start
```

7) After Tomcat and the Secure Alerts server have been restarted, you can log on to the Management Sever by using the Client application to continue managing your firewalls. No certificates need to be reissued because they have been restored from the backup.

Restore a primary Management Server

Restore a High Availability (HA) primary Management Server that has failed completely.

If you have two Management Servers that are configured as an HA pair and the primary Management Server has a complete failure, refer to the following high-level steps to recover from this event.

Steps

1) Using the Client application, log on to the backup Management Server.

   You are prompted to switch this backup server to be the primary server. If you choose to do so, the backup server is promoted to the primary server and, after a brief period of time, you are logged on to the Client application. If you choose not to change the role, you cannot proceed.

2) Remove the High Availability (HA) feature from the backup server by running the **High Availability Removal Wizard**.

   The HA feature will be removed from this server. At this point, you no longer have a primary server. You have a standalone server that was your original backup server. From this point forward in this procedure, this server will be referred to as the old server.

3) Verify the removal wizard successfully removed the HA feature.

   a) The removal wizard generates an haStop.log log file. View the contents of this log file in the **Server Logs** window.

      If you see information at the end of this log that indicates something other than that the configuration completed, the removal wizard was not successful.

   b) If the previous step was unsuccessful, you must troubleshoot this problem.

      Go back to the **Control Center** tree of the **Control Center** icon for the old backup server and try to run the **High Availability Removal** wizard again.

      If it is not available to you (that is, you see the **High Availability Setup Wizard** tree node as opposed to the **High Availability Removal Wizard tree** node), you must contact technical support.

4) Create a new Management Server (hereafter referred to as the replacement server) to replace the failed primary server by reinstalling the Management Server software and ensuring that any applicable patches are in place.

5) On the old server, run the **High Availability Setup Wizard** and specify the replacement Management Server as the backup server.

   You must run the **High Availability Setup Wizard** from the old server and *not* from the replacement server because the old server has the current management data. If you run the **High Availability Setup Wizard** from the replacement server, the old server's data will be lost. At that point, you will need to restore your data from a full backup.

6) The last step depends on whether you want to make the replacement Management Server the new primary server or keep the old server as the new primary server.

   - To switch server roles and make the replacement Management Server the primary server, log off the old server and log on to the replacement server. You are asked whether to make this server the new primary server. Click **OK**. The Switchover Confirmation dialog box is displayed. Select the**Switchover to Secondary Server** checkbox and click **Switchover**. You now have a new primary server with your old server resuming its backup role.
   - To maintain the current backup role of the replacement server as it has been configured by the **High Availability Setup Wizard**, no additional steps are required.

Restore a backup Management Server

Restore a High Availability (HA) backup Management Server that has failed completely

Before you begin

In this scenario, the primary Management Server in an HA pair is running. However, the backup Management Server has failed completely. You want to add a new backup Management Server to your HA pair.

Steps

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

1) Verify the removal wizard successfully removed the HA feature.

   a) The removal wizard generates an haStop.log log file. View the contents of this log file in the Server Logs window.

      If you see information at the end of this log that indicates something other than that the configuration completed, the removal wizard was not successful.

   b) If the previous step was unsuccessful, you must troubleshoot this problem. Go back to the Control Center icon for the old backup server and try to run the **High Availability Removal Wizard** again.

      If it is not available to you (that is, you see the **High Availability Setup Wizard** tree node as opposed to the **High Availability Removal Wizard** tree node), you must contact technical support.

2) Create a new backup Management Server (hereafter referred to as the replacement server) to replace the failed backup server by reinstalling the Management Server software and ensuring that any applicable patches are in place.

Result

Go back to the primary Management Server and run the **High Availability Setup Wizard** in the Control Center icon, specifying the replacement server as the backup server.

Restore both Management Servers in an HA pair

Restore both Management Servers in a High Availability (HA) pair that have failed completely.

In this scenario, both of the Management Servers in your HA pair have failed completely. You can restore a full backup by using the **Upload Backup Wizard** from the **Restore System from Backup** window.
The following procedure is a combination of user interface and command-line steps.

Steps

1) On the new primary Management Server, install the Management Server on the device, including patch information.

2) On the new backup Management Server, install the Management Server software on the device, including patch information.

3) On the primary Management Server, retrieve the backup data. From the command line, log on to the new primary Management Server as `Administrative user` and specify the following commands:

```
cd /tmp
```

```
sudo /usr/sbin/backuptool download -f filename -s scheme -h hostname -d remote-directory -u username -p password
```

where

filename	file name of archive file
scheme	one of FTP,FTPS,SCP
hostname	host name [:port (optional)] (When using FTPS, port is either 21 or 990. Consult your FTP server documentation.)
remote-directory	directory on the host
username	username on the host
password	password on the host

4) Stop all Client applications, Tomcat, and Secure Alerts because open database connections will interfere with the restore process.

To stop Tomcat:

```
sudo /etc/init.d/tomcat stop
```

To stop Secure Alerts:

```
sudo /etc/init.d/dcserver stop
```

5) Restore the retrieved backup data to the primary Management Server by specifying the following commands:

where

`[.des3]`	Optionally use to encrypt file during backup and decrypt during restore.
`[-k passphrase]`	Optionally use the specified passphrase to encrypt the backup file.
`[-L]`	Excludes files in `/var/cc/audit` from the backup or restore operation
`[-D]`	Excludes files in `/var/cc/backups/server/cfgbackups` and in `/var/cc/backups/server/nightlybackups` from the backup or restore operation
`[-b]`	Treats the backup file as having been created on a CC HA system

6) After successfully restoring the backup file, you should start Tomcat and the Secure Alerts server:

To start Tomcat:

```
sudo /etc/init.d/tomcat start
```

To start the Secure Alerts server:

```
sudo /etc/init.d/dcserver start
```

7) On the same (primary) Management Server, run the **High Availability Setup Wizard**. (In the **Control Center** tree of the **Control Center** icon, double-click the **High Availability Setup Wizard** node. The wizard starts.)

Result

When the wizard has completed, the HA feature will have been configured on your two Management Servers.

Create a Management Server backup

Create a new backup or replace an existing backup of your Management Server data using the Client application.

If a failed backup file or a scheduled backup file is selected in the **Existing Backups** table and you click **Replace**, you can specify a new backup name and description and the new backup will replace the previously saved backup.

The resulting backup file can be restored by using the **Restore System from Backup** window.

Note: If configuration domains have been activated, only those users with configuration domain administrative privileges have access.

Steps

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

1) In the navigation bar, click the **Control Center** icon.

2) In the **Control Center** tree, click the **Maintenance** node.

3) Double-click the **Backup System** node. The **Backup Control Center System** window is displayed.

Restore the Management Server configuration files from a backup file

You can restore the operation of the Control Center Management Server to the configuration that was in effect when the backup file was created.

Restore a configuration backup file

Restore a Control Center backup configuration file.

CAUTION: Restoring a configuration will completely overwrite the current Control Center configuration. Exercise caution when requesting this action. E**nsure that no other users are logged on to the Management Server when you are restoring a previously saved configuration.** This action forces all users that are currently logged on to the Management Server to log off.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, expand the **Maintenance node**.

3) Double-click **Restore System**. The **Restore System from Backup** window is displayed.

4) Click anywhere in the row of the backup file to restore and click **Restore**.

> **Note:** If the is backup file is located on a remote server, the **Remote Username and Password** window is displayed.

5) If you need to change the logon information (that is, it has changed since this configuration backup file was saved), do so now. Otherwise, click **OK**. A verification message is displayed.

6) Click **OK**. A message is displayed, indicating whether the restoration was successful or unsuccessful.

7) Click **OK**. If this was a successful restoration, a warning message is displayed, indicating that all users who were previously logged on to this Control Center Client icon will be logged off, including you. You will need to log on to the Control Center again. If this was an unsuccessful restoration, resolve the errors and then try this procedure again.

Edit a system backup file

Edit a backup configuration file.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, expand the **Maintenance node**.

3) Double-click **Restore System**. The **Restore System from Backup** window is displayed.

4) Double-click the file to edit. The **Backup Details** window is displayed.

5) Make your changes.

6) To save your changes, click **OK**.

7) Repeat the Steps 4 - 6 as needed.

8) When you have finished, click **Close**.

Delete a system backup file

Delete a system backup file.

> **Note:** The Initial Configuration backup file cannot be deleted.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, expand the **Maintenance node**.

3) Double-click **Restore System**. The **Restore System from Backup** window is displayed.

4) Click the row to be deleted and click **Delete**.

5) A confirmation message is displayed. To continue with the deletion, click **Yes**. Otherwise, click **No** to cancel the deletion.

Upload a backup configuration file from the Client to the Management Server

Use the **Upload Backup Wizard** to identify a Management Server configuration file that is stored locally on the Client machine and make it available to use in a restore operation.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, expand the **Maintenance** node.

3) Double-click the **Restore System** node. The **Restore System from Backup** window is displayed.

4) Click **Upload**. The **Upload Backup Wizard** is displayed.

5) Complete the wizard. The uploaded backup appears on the **Restore System from Backup** window.

Change logon information for remote system backups

Access the **Remote Username and Password** window when you are attempting to restore a configuration file for the Control Center Management Server that is stored on a remote server and the logon information for that server has changed since this file was saved.

When this window is displayed as part of the restoration process, you can change the information to match the current logon information for the remote server.

Note: This procedure assumes that you have already created a remote backup configuration file.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, expand the **Maintenance** node.

3) Double-click the **Restore System** node. The **Restore System from Backup** window is displayed.

4) Highlight the remote backup file (that is, a file that has a URL in the URL field) and click **Restore**. The **Remote Username and Password** window is displayed.

Starting and stopping the Management Server

You can restart the Control Center Management Server from within the Client application by double-clicking the **Restart Server** node under the **Maintenance** node of the **Control Center** tree in the Control Center icon.

If you select **Yes**, the server will be restarted *immediately*. There is no second confirmation request.

You can also stop the Management Server and exit the application by double-clicking the **Halt Server** node. Then click **Yes** to confirm or **No** to cancel the action. There is no separate window for this action.

Restart the Management Server

Restart the entire Control Center Management Server. When the restart begins, the Client application will exit and all pending connections will be closed.

> **Note:** If you perform a restart to invoke new server properties, only the Management Server application will be affected, not the entire server.

Steps

1) In the navigation bar, select **Control Center**.

2) In the **Control Center** tree, expand the **Maintenance** node.

3) Double-click the **Restart Server** node.

4) Click **Yes** to restart the server.
If you click **Yes**, the server will be immediately restarted. There is no second confirmation request.

CHAPTER 37

Control Center administrators

Contents

The tasks that can be performed by administrators are determined by the assigned role and the specific firewalls over which an administrator can have authority.

About Control Center administrators

Each administrator who can log on to the Control Center must be identified and authenticated.

This is accomplished by specifying a unique user name and password for each administrator. There are two different ways to do this:

- In the Control Center Client application, specify the required authentication values for the administrator in the **Control Center Administrator** window. The authentication information is stored on Control Center.
- If you are using an LDAP server to manage your user accounts, specify the required authentication values in the LDAP user account on the LDAP server. Assign this user to a user group on the LDAP server. On the Control Center Client application, create an LDAP user group that represents the user group on the LDAP server. The authentication information is stored on the LDAP server.

Use the **Control Center Administrator** window to specify Control Center administrators. These windows are used to perform the following tasks:

- Create and manage the Control Center administrator accounts.
- Assign previously defined roles to an administrator.
- Specify the firewalls that can be accessed by the named administrator.
- Restrict the time of day and days of the week that administrators can log on to the Control Center.
- Specify when access to the Control Center expires.
- Specify if and when an administrator is required to re-authenticate after a specified amount of inactivity (lack of mouse movement).

Use the **Role** window to specify the roles that are assigned to Control Center administrators.

If configuration domains are activated, the **Domain Access** tab is displayed, where you can specify the domains that the administrator can log on to and the privileges that he or she has for configuring and managing the domain.

If external, off-box authentication is selected, you can select a failover internal authentication method for an administrator. If you select the **Allow authentication fallback** checkbox, credentials that have been submitted to log on to the Management Server from the Client are presented to the internal authentication system if there is a communication failure between the Management Server and the off-box authentication server (LDAP or RADIUS).

Note: The Control Center Administrator window is not used to configure administrators who are authorized to directly manage security devices, such as firewalls, or to pass data through a firewall.

Related concepts
Authentication services on page 115
Advantages of configuration domains on page 499

Configure Control Center administrators

You can manage Control Center administrator accounts in the **Control Center Administrator** window.

When you add administrators in this window, they are able to log on to the Control Center Client application to manage objects from a central location. You cannot use this window to configure or manage administrators who have access to specific firewalls.

Steps

1) In the navigation bar, select **Control Center**.

2) Double-click the **Administrators** node. The **Control Center Administrator** window is displayed.

3) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

4) Click **OK** to save this object.

Control Center passwords

You can change the passwords of other users in the **Control Center Administrator** window. However, to change your own password, use the **Change User Password** window.

Change user passwords

Use the **Change User Password** window as an alternate way to change your user password.

This window is available only if your user profile has been configured to use internal authentication to access the Control Center (as opposed to external authentication).

If you have administrator privileges and you want to change the password of a different user, use the **Control Center Administrator** window.

Steps

1) In the title bar of the main window, click **Change Password**. The **Change User Password** window is displayed.

2) Configure the fields on this window as needed.

   Note: For option descriptions, press **F1**.

3) Click **OK** to save this password.

CHAPTER 38

LDAP user groups

Contents

LDAP user group functionality simplifies maintenance of administrative users between the LDAP server and Control Center. As users are added to or removed from groups on the LDAP server, they are automatically enabled or disabled on the Control Center Management Server when synchronization of the databases occurs.

About LDAP user groups

An *LDAP user group* is a representation of a group of administrative users who have already been defined as part of an administrative group on an LDAP server.

The important difference is that these administrator accounts can be synchronized with user group accounts on the LDAP server or dynamically created when the administrator, who is a member of one of these LDAP user groups on the LDAP server, but who is not defined on the Control Center, attempts to log on to the Client application.

In other words, the user accounts and groups must still be created on the LDAP server. However, they do not have to be created *again* on the Control Center Client application. Only the LDAP user group objects must be created. When the user attempts to log on to Control Center, after checking the existing Control Center administrator accounts, the LDAP user groups are checked. If the credentials of this user match one of the LDAP user groups, he or she is allowed to log on to Control Center and an administrator object is dynamically created for him or her.

Create LDAP user groups on Control Center

Use the **LDAP User Group** window to configure LDAP user groups.

You create the group in Control Center that matches the LDAP user group that has been configured on the LDAP server. In this window, you configure the attributes and privileges for this group.

Steps

1) In the navigation bar, select **Control Center**.

2) Double-click the **LDAP User Groups** node. The **LDAP User Group** window is displayed.

Import LDAP administrator accounts into Control Center

Use the **Import Administrator Accounts** window to import new administrator accounts into Control Center from the LDAP server.

Before you begin

You must have completed the following to access this window:

- You must have created at least one LDAP user group.
- You must have already configured LDAP authentication on the **Authentication** window.

After the LDAP server is queried for the members of the selected group, you have the option to include or exclude any members of this group to be imported into Control Center at one time. Note that these members will still be able to log on in the future as long as they remain members of this group on the LDAP server. A possible use of this window is to import particular members so that you can provide special configuration of their accounts.

Steps

1) In the navigation bar, select **Control Center**.

2) Expand the **LDAP User Groups** node.

3) Right-click the group object for which you want to import accounts and select **Import Administrator Accounts**. The **Import Administrator Accounts** window is displayed.

Using LDAP user groups to create administrator accounts on Control Center

The following sections provide high-level information about the entire process for configuring LDAP user groups and also the process that Control Center uses to authenticate users who are members of LDAP groups.

LDAP user group configuration process

Perform these high-level tasks to configure a LDAP user group.

1) On Control Center, configure LDAP as the external authentication method on Control Center.

2) On the LDAP server, create all your user accounts and user groups. Arrange the members of the groups as desired.

3) On Control Center, create an LDAP user group.

4) Import the members of the group on the LDAP server into the LDAP user group on Control Center.

5) [Optional] Configure the time period at which the Control Center will query the LDAP server to verify administrator accounts. This is done on the **Authentication** window.

User authentication process

With the implementation of LDAP user groups and LDAP authentication, an additional layer has been added to the authentication processing on Control Center.

1) The user attempts to log on to the Control Center Client application.

2) The external authenticator is searched for the user account

3) The Control Center Client application performs a search in its database to find the corresponding user account.

4) Without LDAP user groups, if no account match is found, the log on attempt is rejected. With the implementation of LDAP user groups, the Control Center Client application attempts to log on to the LDAP server

5) If the password for the server is invalid, the user will be denied access to the Control Center Client application.
or

   If the password is valid, the Control Center Client application will query the LDAP server to obtain all the attributes that are associated with this user.

6) If there is at least one attribute match with a user group on the LDAP server, the user will be able to log on to the Control Center Client application. A dynamic administrative account will be created for him or her at that time on Control Center. Therefore, the user can log on whether he or she has an administrative account already configured on Control Center or not—as long as he or she is a member of that configured LDAP user group.
or

   If there are no attribute matches, the user will not be able to log on to the Control Center Client application.

Related concepts
Configuring LDAP authentication or RADIUS authentication on page 454

CHAPTER 39

Control Center roles

Contents

Use roles to restrict the actions that users can perform on the Control Center.

About Control Center roles

A role defines the activities that a user is permitted to perform on each type of object in the Control Center, and the actions that the user is allowed to perform across the various tools.

The objects include, but are not limited to, endpoints, services, firewall users, time objects, VPNs, and certificates. The activities are defined as:

- **View** — The user can view objects.
- **Update** — The user can update existing objects.
- **Add** — The user can add new objects.
- **Remove** — The user can remove objects.

You can use roles in many different ways to add strong security when you are configuring firewalls. For example, your organization can require that the action of two or more users must be involved to administrate a firewall. Each user would need to contribute his or her part of the configuration before a complete configuration can be created and applied. For example, you can create a role that allows a user to have full access to all objects, except for those that are used for VPN. You can create another role to allow a user to have access only to the objects that are used for VPN (for example, VPN peers, communities, and certificates). To create a firewall configuration that employs VPN, the actions of both users would be required.

You can also configure an environment that uses permitted actions by specifying a role in which one user can specify and validate configurations, and by specifying another role to allow a different user to apply configurations.

You can create any number of roles and you can assign any number of roles to a user. If you have assigned a role to a current user, the role cannot be deleted.

Use the **Role** window to create roles that can be assigned to Control Center users.

The following roles are defined by default. However, you can delete any of these roles except for the Administrator role (again, if it is not assigned to a current user):

- **Administrator** — This is an administrator with full access to all object types. This is the only predefined role that cannot be deleted.
- **VPN Administrator** — This is an administrator who can manage VPN access.
- **Audit and Alert Administrator** — This is an administrator who can manage audits and alerts.
- **Audit and Alert Monitor** — This is a user who can view and manage firewall alerts and activities, and who can also view reports from firewalls.

Use the **Control Center Administrator** window to assign these roles to users.

Related tasks

Configure Control Center administrators on page 490

Manage roles for Control Center users

You can manage roles that can be assigned to Control Center users in the **Role** window.

In addition to role assignment, you can also configure the objects that this user can access and the actions that can be performed on these objects.

Steps

1) In the navigation bar, select **Control Center**.
2) In the Control Center tree, double-click the **Roles** node. The **Role** window is displayed.
3) Configure the fields on this window as needed.

   Tip: For option descriptions, press **F1**.

4) Click **OK** to save the object.

CHAPTER 40

Configuration domains

Contents

Configuration domains are used to partition managed firewalls into separate collections of objects and configuration data so that each collection is independent of every other collection, and changes to one collection do not affect others.

Advantages of configuration domains

There are two main advantages for creating configuration domains.

- By using multiple configuration domains, administrator responsibilities can be segregated to allow each administrator (or group of administrators) to have control of the firewalls and their related objects for a single domain.
- When a configuration domain administrator logs into the Control Center, he or she sees and acts on only those objects that are related to the configuration domain that he or she is currently logged on to. Information about other domains is not visible.

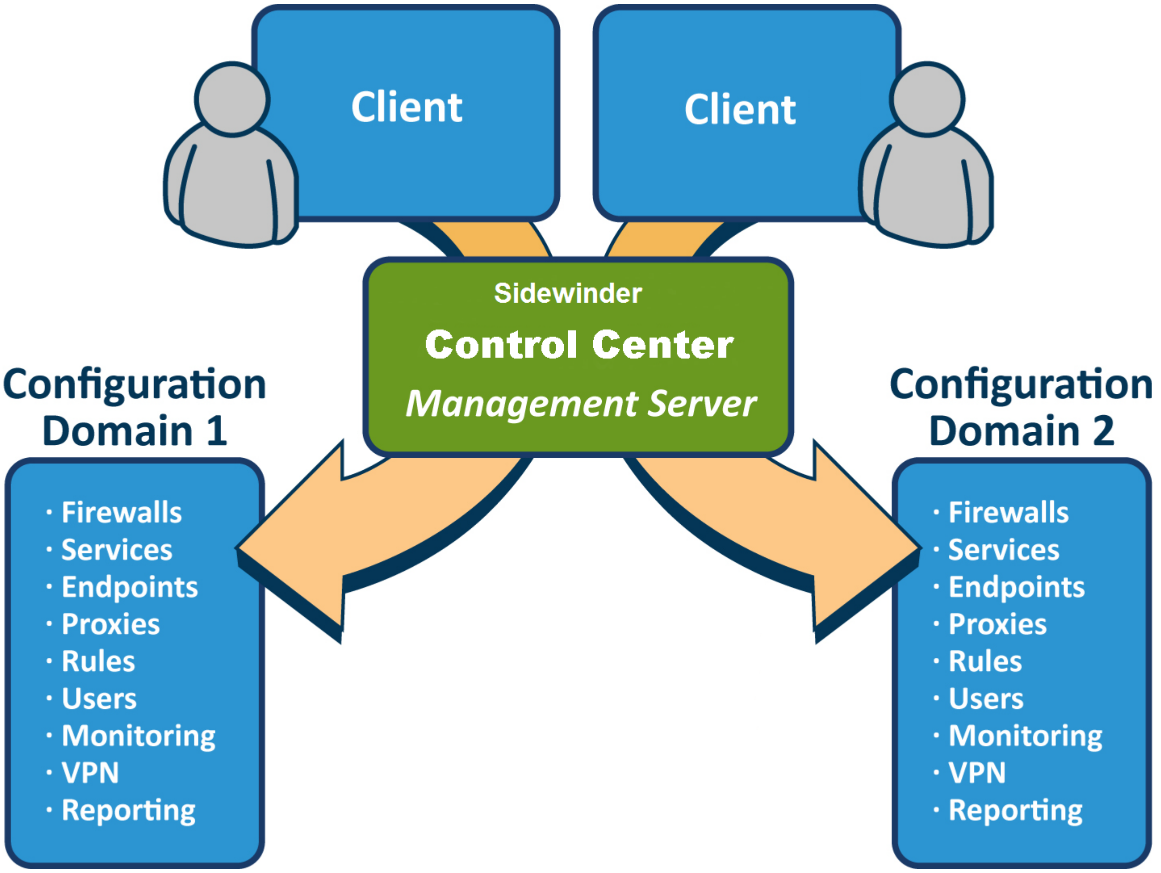
If you use configuration domains, you can compare it to having multiple installations of the Control Center, with each installation having independent control over a domain and all the associated, domain-specific data. The main difference is that all the data for all the domains is managed by a single Control Center Management Server.

When you log on to the Client application, a specific configuration domain is selected. Only those objects that belong to the selected domain are visible for the duration of that session. You can change domains in the Domain field in the tab area of the main window.

Configuration domains define the firewall and object operations that an administrator can manage, configure, report on, and monitor when he or she is logged on to that configuration domain. Additionally, the administrator function is further defined according to the privileges (roles) that he or she has been assigned for that domain.

A single Control Center installation can support multiple domains by keeping separate from all the other domains those firewalls, objects, and configuration data that are associated with each domain. Administrators can switch from domain to domain by selecting a different domain at the logon page.

Figure 28: Single Control Center supporting multiple domains



For customers who are not interested in segmenting responsibilities into separate domains, the Control Center supports all the management features, configurations, and functions in a single domain environment that is completely transparent to the administrator.

Most of your environments that are supported by the Control Center will not require the additional support and user/role management that is required to support configuration domains because you are managing firewalls that are associated with a single, enterprise-class domain.

Activating configuration domains

After you install the Control Center Management Server and Client application for the first time, a single domain configuration is configured. The mechanisms and conventions that are associated with having multiple configuration domains are transparent when you are in this mode.

You must use the functions that are in the Control Center icon to create additional configuration domains.

To activate the configuration domain option, you must configure a second configuration domain.

After the second domain has been created, the creator of this domain is notified that from that point going forward, only those Control Center users who have administrative privileges for that configuration domain can access the Client application.

By activating a configuration domain, a new class of Control Center user called the configuration domain administrator is created. Each Control Center user who is a member of the Administration Domain is a configuration domain administrator. Only those Control Center users with this privilege can:

- Log on to the Control Center Client application.
- Create and destroy configuration domains.
- Create, modify, and delete Control Center users (administrators) and manage their associated roles for each domain.
- Manage system-wide settings.
- Configure and manage external authentication.

By default, the creator of a configuration domain is granted administrative privileges for the configuration domain and is a member of the administration domain.

All other Control Center users must be configured to determine the following actions:

- The domains to which they have access
- The roles that determine the objects that they can manage and the actions that they can take.
- Whether they have administrative privileges for the configuration domain so that they can log on to the Client application.

After initially activating configuration domains, the appearance of the Control Center Client application main window changes to accommodate the new functions that are required to manage user access to specific domains. Specifically, the **Domain** field is now displayed in the tab area of this window.

The following domains are displayed on the **Domain Access** tab of the **Control Center Administrator** window:

- Shared
- Default
- Administrator
- *<User-created domain>*
  Where the *User-created domain* is the newly created configuration domain that activated the configuration domain option.

Two of the domains are special-purpose domains that have been created:

- Administrator domain
- Shared domain

Administrator domain

Use the administrator domain to identify those users who have administrator privileges for the configuration domain. All users who will be allowed to access the Client application need to be activated in the administrator domain.

Shared domain

The shared domain contains all the common objects that are shared across all the configuration domains. This includes a set of default, generic configuration objects that are used to perform a variety of functions that are configured when the Control Center was initially installed.

To work with objects in the shared domain, an administrator must be explicitly permitted access to log on to the shared domain. If you add an object to the shared domain, this object is universally available to all the configuration domains that are defined in the Management Server.

Conversely, if you change the characteristics of an object in the shared domain, the object characteristics are changed in all configuration domains. Make sure that you carefully consider this when you decide to change the characteristics of any object in the shared domain. Otherwise, this change can cause problems across multiple domains that use this same object. A good practice is to copy an existing object in the shared domain, rename it, change the specific characteristic or characteristics and save the change. This new object can be accessed by all users.

The shared domain has special limitations. Firewall objects may not appear in the shared domain. Objects in the shared domain may not reference objects in a non-shared domain.

Certain objects contain "apply on" attributes that reference firewalls. The shared domain can support those objects with empty "apply on" associations.

Although objects in the shared domain are visible when you edit a configuration domain (shared object are green) and it is possible to reference the shared object from within the configuration domain, you cannot change the characteristics of the shared object while you are editing object data in a configuration domain. However, you can copy the shared object. The copy will reside in the configuration domain and it can then be fully characterized.

Objects cannot be moved from a shared domain to a configuration domain, or moved or copied from a configuration domain to the shared domain.

Because the shared domain does not exist unless configuration domains have been activated, sites that do not use activate configuration domains will not have a shared domain.

Managing configuration domains

You can create new configuration domains or editing existing domains in the **Configuration Domain** window.

You can also move firewalls or cluster nodes between configuration domains and switch between domains.

Configure configuration domains

You can create new or edit existing versions of configuration domains in the **Configuration Domain** window.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, double-click **Configuration Domains**. The **Configuration Domain** window is displayed.

Move a firewall or cluster from one configuration domain to another

You can move a firewall or cluster from one configuration domain to another domain as long as you have administrative privileges in both domains.

The following procedure is a high-level overview of the steps that are required to move a firewall or a cluster from one configuration domain to another configuration domain.

Steps

1) In the Client application, log on to the source domain (for example, Domain A). (This is the domain from which you want to move the firewall or cluster.)

2) Make sure that the **Firewalls** tab is selected.

3) Expand the **Firewalls** node or **Clusters** node, depending on the object that you are moving.

4) Right-click the firewall or cluster node to be moved and select **Remove** Object.

5) If there are no other versions of this configuration domain (Domain A), skip to Step 6. or If there are other versions of this domain, repeat Steps 1—4 until the firewall or cluster is removed from all the Domain A versions.

6) Log on to the target configuration domain (for example, Domain B).

7) Right-click on either the **Firewalls** or the **Clusters** node (depending on the object that you are moving) and select **Add Object**. The **Add new firewall** window or the **Add Cluster** window is displayed, depending on the node that you selected.

8) Specify the information necessary for the object that you are moving and click **OK**. The object is added to the respective node.

Change from one configuration domain to another

Use the **Domain field** list in the tab bar to change between configuration domains, provided that you have access to each of these domains. You can switch domains without having to log off and on again or re-specifying your user name or password.

Note: This field is available only if configuration domains have been configured.

Configuration domain version management

With the advent of configuration domains comes the concept of saving a version of a configuration domain that is separate from and distinctly different than a backup configuration of the Management Server.

Multiple versions of a domain can be captured. While only one domain version may be active at any time, any previously saved version can be activated at any time. The active domain is the domain that currently governs the security policy for the specific domain. When changes are made to a domain configuration, the changes are saved for the currently active domain. By default, when a user logs into the Client application, he or she logs into the active version of the domain.

By supporting multiple domain versions, you can have the flexibility to change a security policy to a pre-configured (and previously saved) version. By creating a saved version of a current configuration, you can make configuration changes to the active version without worrying about how to recover if the policy is flawed or if the backup does not proceed as planned. To recover, you can activate the previously working configuration.

To create a domain version, name the version and save the configuration. Note that saving a domain version does not activate it. Activating a domain version is a separate process. When a new domain version is activated, you, and any other administrators who are logged on to any tools that use the current domain, will be logged off and all you will be required to log back into the Control Center.

You can also manage the various versions of configuration domains in the **Configuration Domain Version Manager** window.

Related tasks

Managing configuration domains on page 502

Saving versions of configuration domains

If configuration domains are activated, use configuration domain version management to save and activate backup configuration data that is associated with each individual configuration domain.

Saving a version of a configuration domain is separate from and distinctly different than saving a backup configuration of the Management Server. In many ways, this process accomplishes the same goals as a system backup. However, it differs in a few key areas that are important to understand.

The first difference is that there is no mechanism and there is none required to FTP a version of a configuration domain to an off-box location. All the versions of all defined configuration domains are saved during a normal Control Center Management Server backup procedure that can be stored in an off-box location to support worst-case failure recovery scenarios.

The next major difference is that only the configurable data that is associated with the specific configuration domain is preserved. No shared domain data is preserved. Although judicious management of shared objects should prevent shared object characteristics from being altered in any way that might cause problems when used with a configuration domain configuration, shared object configuration characteristics are not preserved with the configuration domain object characteristics.

Multiple versions of a domain can be captured. Although only one domain version can be active at any time, any previously saved version can activated at any time. The active domain is the domain that currently governs the security policy for the specific domain. When you make changes to a domain configuration, the changes are saved for the currently active domain. By default, when you log on to the Client application, you log on to the active version of the domain.

Manage versions of configuration domains

You can manage different versions of configuration domains in the **Manage Configuration Domain Versions** window.

By supporting multiple domain versions, you have the flexibility to change a security policy to a pre-configured (and previously saved) version. By creating a saved version of a current configuration, you can make configuration changes to the active version without worrying about how to recover if the policy is flawed or if the backup does not go as planned. You can activate and apply the previously working configuration.

By saving different versions of configuration domain configurations, you can configure alternate security policies that can be quickly activated.

To create a domain version, use the **Manage Configuration Domain Versions** window to assign a name to identify the version and save the configuration. Note that the act of saving a domain version configuration does not activate it. Activating a domain version is a separate process.

To activate a previously saved version of a configuration domain, use the **Manage Configuration Domain Versions** window to highlight the version to activate and click **Activate**. When a new domain version is activated, you and any other administrators who are logged on to any tools that use the current domain are logged off and all you will be required to log back into the Control Center.

It is easy to manage versions of a configuration domain, provided that you exercise good configuration change practices. For example, if some configuration changes are going to be implemented to a configuration domain, use the following practices to assure success if the changes are successful or not:

- Before you make major changes to the objects in a configuration domain, save the current configuration. If you are not certain that the configuration in the Management Server database matches the configuration of the managed firewalls, generate compliance status data to verify that the configuration on the managed firewalls corresponds to the configuration data that is stored in the Management Server. When you are satisfied that the Management Server data is correct, save a version of the configuration data. Remember that saving a version of the current configuration does not activate the newly saved version. This newly saved version represents a known good configuration that can be activated in the very near future if the configuration changes that are about to be made do not have the desired effect or if they need to be backed out.
- Make your configuration changes by using the features and functions of the Control Center icon. Remember that all the changes are being saved in the currently active version of the configuration data. It is always good policy to validate changes before applying them by running the **Validation Status** report. When you are satisfied with the validation data, apply the changes.
- To see information about the status of the propagation, access the **Configuration Status** page by selecting the **Configuration Status** tab in the **Policy** icon.

Observe and test the operation of the newly applied configuration data. If all has gone well, the backup configuration is no longer required. It can be saved or deleted. If the configuration changes do not operate as expected, the backup configuration can be activated and applied to restore the known good configuration.

To access the **Manage Configuration Domain Versions** window:

From the navigation bar:

Steps

1) Select **Control Center**.

2) In the Control Center tree, expand the **Configuration Domains** node.

3) Right-click the configuration domain object to manage and select **Manage Versions**.
   From the main window when configuration domains are enabled:
   Click **Manage versions**, which is located to the right of the **Domain** list in the tab area of the main window.

CHAPTER 41

Log files and the Support Tool

Contents

Log files provide audit information about the Control Center. The **Support Tool** bundles these log files with configuration and system information to provide Forcepoint support the information needed to resolve issues quickly.

Viewing Management Server logs

You can view various types of Control Center Management Server log files that are consolidated into one window the **Server Logs** window.

You can also configure the logging settings of the Control Center Management Server in the **Control Center Server Log Configuration** window.

You can view information about the Control Center Management Server on the **System Information** window.

View log files

Access the Server Logs window.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, expand the **Logs** node.

3) Double-click the **Server Logs** node. The **Server Logs** window is displayed.

4) From the log groups, select a log to view details. The right window displays the log information. You can search for specific text in the log file.

5) You can wrap long lines, set fonts, specify lines to be shown in the log file.

6) Click **Export** to save the log file in plain text format to the system.

Configure logging settings on the Management Server

Access the **Control Center Server Log Configuration** window.

Steps

1) In the navigation bar, select **Control Center**.
2) In the **Control Center** tree, expand the **Logs** node.
3) Double-click the **Server Logs** node. The **Server Logs** window is displayed.
4) Click **Settings**. The **Control Center Server Log Configuration** window is displayed.
5) From **Logging Level**, specify the amount of log information to be collected. You can select **Basic**, **Standard**, or **Verbose** level.
6) In **Number of logs to keep**, set the number of logs to be retained. The default value is 10 and maximum limit is 20.
7) Set the maximum size of each log size in MB. The maximum limit is 100 MB.
8) Click **OK** to save these log settings.

Display system information for the Control Center Management Server

View information about the Control Center Management Server.

Steps

1) In the navigation bar, select **Control Center**.
2) In the Control Center tree, expand the **Logs** node.
3) Double-click the **System Information** node. The **System Information** window is displayed.

Tip: For option descriptions, press **F1**.

Viewing cryptographic logs

The **Crypto Log** page is used to view and analyze the Control Center cryptographic activity that is stored on the Management Server.

You can review cryptographic activities that are performed by a specific user or audit all the cryptographic activities that occurred in a specific time frame.

View cryptographic activities

View cryptographic logs for the Control Center.

Steps

1) Navigate to **Control Center** > **Logs** > **Crypto Logs**. The **Crypto Logs** page is displayed.

   Tip: For option descriptions, press F1.

2) Use the filter and find fields to quickly identify cryptographic activities that are of interest.

   Tip: Click a column heading to sort the table by the information in that column.

About the Support Tool

The **Support Tool** is an application that can be run from the command line or accessed in the user interface from the **Control Center** tree of the **Control Center** icon. This application combines log files, configuration files, and system information into one file (configuration bundle) that can be provided to technical support to assist with troubleshooting.

Providing configuration files for technical support

The **Support tool** makes it easier to provide this information to technical support if they need to help you to resolve an issue. In addition to creating this file on the Control Center Management Server appliance, you can also export it from the Control Center Management Server to a local system.

Create the support file

Create the support file to provide Forcepoint support with additional information regarding your issue.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, double-click the **Support Tool** node. The **Support Tool** window is displayed.

3) Enter the Service Request number in the **Service Request number** field.

4) If you want to include database backup files, select the **Include database backup** checkbox.

5) Click **Create Support File**. A message is displayed, indicating that the support file has been created, along with its path and file name on the Management Server. This file is always created in the following directory:

   `/var/cc/support`

   Each file name is created in the following format: SR + the **Service Request number** field value + .tar + .gz. An example is SR123456789.tar.gz.

6) Click **OK** to return to the **Support Tool** window.

7) If you want to export this file to a local system, click **Export**. When the exportation has completed, a **Download Complete** message is displayed, which also includes a checksum for this file.

8) Click **OK**.

Create the support file from the command line

In addition to being able to access this tool through the Client user interface, you can also use the command line to create the support file.

Steps

1) Log on to the Control Center Management Server console as the `Administrative` user.

2) Run the Support Tool (`support_tool`) command by using any or all the parameters that are listed below.

```
sudo /usr/sbin/support_tool [-cdlmnrsSt] filename
```

   where: *filename* is the name of the file in which the results are placed and:

```
-a      = all common options (which is the same as specifying -dlmnrt)
-c      = configuration database backup
-d      = disk space, CPU utilization, and memory usage
-l      = HA logs
-m      = Control Center server logs (cc_log)
-n      = network interface information
-r      = release level and hotfixes or epatches installed on server
-s      = system database backup
-S      = SEM logs
-t      = Tomcat web server logs (catalina)
```

CHAPTER 42

High Availability (HA)

Contents

A High Availability (HA) configuration provides continued firewall management in the event a Management Server becomes unavailable.

About High Availability Management Servers

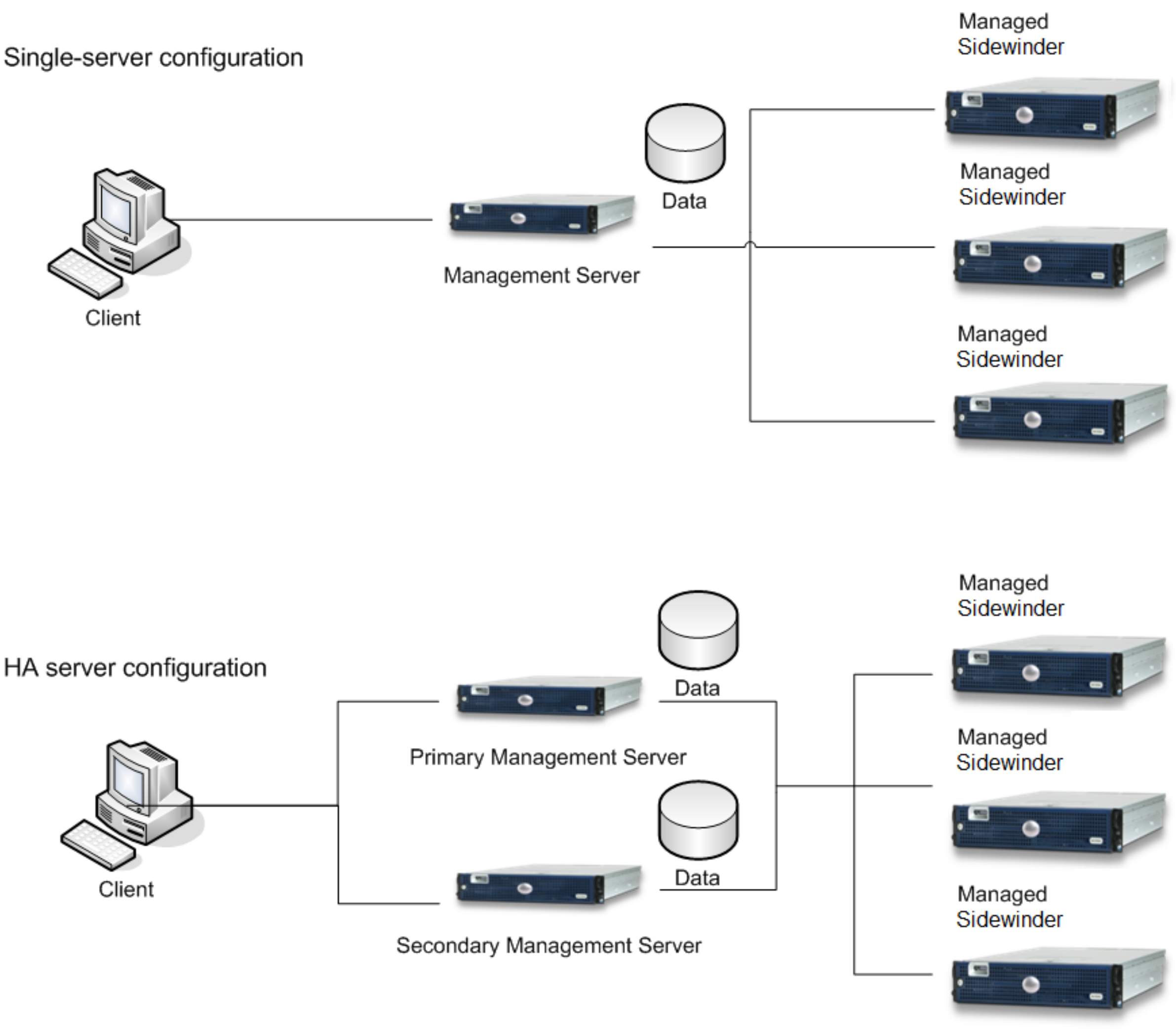
For the Control Center, the High Availability (HA) feature refers to two Control Center Management Servers that are configured to work together to provide redundancy and continuity.

You will designate one server as the primary Management Server and the other as the backup Management Server. The primary and backup server roles can be reversed at any time.

Note: High availability on the firewall refers to firewall cluster configurations. On the Control Center, High Availability refers to Management Server configurations.

The High Availability (HA) Management Server uses this dual-server configuration to continue operations of the Control Center Management Server functions if one Management Server becomes unavailable for any reason. Although the HA Management configuration provides an effective way to maintain operation if a server fails, it is not an automated failover solution. The following diagram illustrates the difference between a single-server configuration and an HA configuration.

Figure 29: High Availability Management Server configuration



Related concepts

About clusters on page 277

How HA Management Servers work

When you configure HA by using the High Availability Setup Wizard, you are prompted to designate the primary Management Server. The other server will become the backup server.

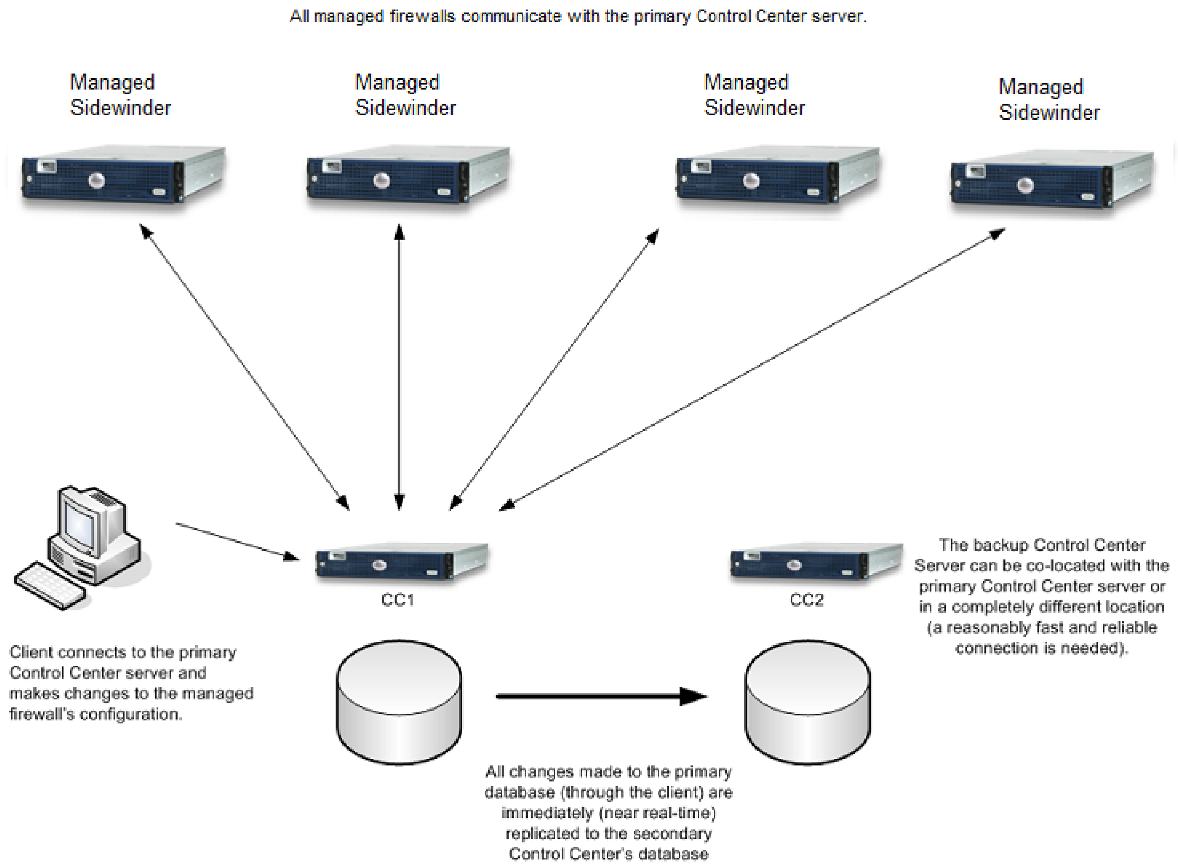
Subsequently, if you log onto the backup server, you are prompted to switch this server to be the primary server. If you agree that this is what you want, the backup server is then designated as the *primary* Management Server.

The primary Management Server manages your security policy in its database. After HA is configured, the database of the backup Management Server is automatically synchronized with the data that is stored in the primary Management Server database. This process is referred to as *data replication*.

Processing with an active primary Management Server

The following diagram illustrates the processing that occurs in an HA configuration when the primary is active.

Figure 30: High Availability process flow with primary Management Server


All managed firewalls communicate with the primary Control Center server.
Managed Sidewinder
Managed Sidewinder
Managed Sidewinder
Managed Sidewinder
CC1
CC2
The backup Control Center Server can be co-located with the primary Control Center server or in a completely different location (a reasonably fast and reliable connection is needed).
Client connects to the primary Control Center server and makes changes to the managed firewall's configuration.
All changes made to the primary database (through the client) are immediately (near real-time) replicated to the secondary Control Center's database

The following legend describes the HA process in this figure:

1) All the managed firewalls are communicating with the primary Management Server only.

2) A user uses the Client application to access the primary Management Server and to make changes to the configuration of one of the managed firewalls.

3) The backup Management Server can be co-located with the primary server or it can be in a completely different location (although a reasonably fast and reliable connection is needed between the two servers).

4) All changes that are made to the database of the primary server are immediately replicated to the database of the backup server.

Signing into a backup Management Server

When a user logs on to a backup Management Server by using the Client application, the next operation depends on the current state of the primary Management Server.

If the primary Management Server is fully operational, a *switchover* is performed. If the primary Management Server is not operational, a *failover* is performed.

Switchover versus failover

A switchover is an orderly transfer of the master database designation from the primary Management Server to a backup Management Server.

During a switchover, the two nodes are constantly communicating to make sure that no transactions are lost. This is the preferred operation.

In a failover, the transfer of the master database designation still occurs. However, the backup Management Server does not wait for acknowledgment from the primary Management Server.

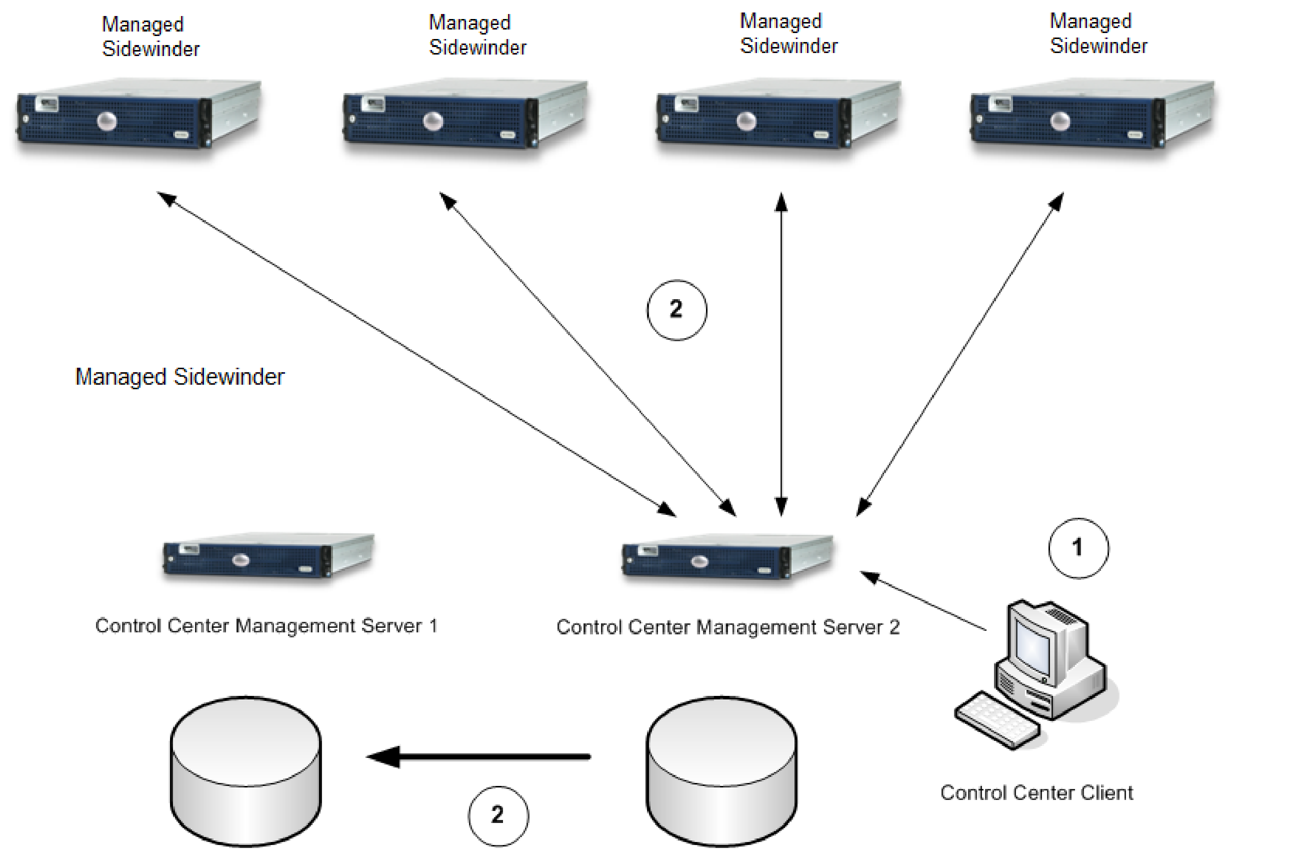
If a user attempts to log on to a backup Management Server, a warning is displayed, indicating that the user is attempting to log on to the backup Management Server. If the user decides to continue, this server becomes the primary Management Server. The previously designated primary Management Server is automatically notified about the change and automatically becomes designated as the backup Management Server.

Replication occurs whenever the database of the primary Management Server is updated. Information is written to the database of the primary server from the Control Center application. The replication subsystem adds these changes to the queue for replication to the database of the backup server. The replication typically happens within seconds of any database change. However, if a failure occurs, the transactions are queued and are then re-sent as needed.

Processing in a failover HA scenario

The following diagram illustrates the processing that occurs in an HA configuration when the primary Management Server fails over to the backup Management Server.

Figure 31: High Availability process flow when the primary Management Server fails over to the backup server



The following legend describes the HA process in this figure:

1) A user logs into the backup Management Server and receives a warning that the backup server will perform a switchover that will make the backup server the new primary Management Server.

2) The new primary server notifies the other server that it now has the master database.
The new primary server starts replicating data from its database to the new backup server after this point in time.

The new primary server will also notify all the managed firewalls that it is now the new primary server.

All changes that are made to the database of the new primary server are immediately replicated to the database of the new backup server.

Configuring HA Management Servers

The purpose of the High Availability (HA) feature is to continue the Management Server processes if the primary Management Server is suddenly unavailable for any reason.

Ensure HA Requirements are met

Before you begin this configuration process, make sure that the following requirements have been met for the two Management Servers to use.

- Before configuring High Availability, external authentication, which is either LDAP or RADIUS authentication, must be turned off for SSH and console logins. You can do this in the **Authentication** window.
  After High Availability configuration is complete (that is, after the **High Availability Setup Wizard** has completed successfully), you can re-enable external authentication on the two Management Servers.
- Both Management Servers must be installed and have proper network communication, which includes standalone port configuration.
  The following table shows a list of TCP ports that are required for HA configuration.

  Table 42: List of TCP port configurations that are required for High Availability between two Management Servers

Port	Description
Port 22	SSH
Port 5432	Control Center Management Server database
Port 9005	Control Center Management Server HTTPS/SSL port

- Both Management Servers must be configured with the same user names and passwords for the following accounts:
  - Control Center administrator
  - Management Server administrator (Administrative user)
- Both Management Servers should have the correct server date and time. Use the **Date and Time** window to set these values.
- Both Management Servers must have a minimum of 100MB of free disk space in the `/opt/security` directory before HA can be configured.

Related reference

Port configurations for network communication on page 25

Configure HA Management Servers

Use the Control Center **High Availability Setup Wizard** to configure the HA feature on two different Management Servers that you designate as a primary and a backup Management Server.

Steps

1) In the navigation bar, select **Control Center**.

2) In the **Control Center** tree, double-click the **High Availability Setup Wizard** node.

3) Complete the wizard.

View additional HA log files

If the backup Management Server was successfully configured with the HA feature, there are two different types of logs that are generated.

Steps

1) Click **Control Center** and expand the **Logs** node, select **Server Logs**. Configuration logs are displayed on the **Server Logs** page in the **High Availability Setup** folder.

2) Click **Control Center** and expand the **Logs** node, select **Server Logs**. Transaction logs are displayed on the **Server Logs** page in the **High Availability** folder.

Troubleshooting tips after a successful removal

If your first attempt to configure the HA feature was unsuccessful, but the configuration was successfully removed, you can use the setup wizard to re-configure it again.

1) Go through the prerequisites above. Make sure that both of the Management Servers meet all these requirements.

2) Start the setup wizard again. (Click **Control Center** and select **High Availability Setup Wizard**.)

Remove Management Servers from HA configuration

The Control Center High **Availability Removal Wizard** removes the HA feature on the primary and backup Management Servers.

If you have a failover state, in which the primary Management Server cannot communicate with the backup Management Server, restore the backup server before removing HA. However, if this is not possible, you can still remove HA, although an error is reported.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, double-click the **High Availability Removal Wizard** node.

   Note: This tree option is available only if you have previously configured the High Availability (HA) feature on two of your Management Servers—that is, one primary and one backup Management Server.

3) Complete the wizard.

Result

After you have successfully run the **High Availability Removal Wizard** on the primary Management Server, there are additional steps that you can take regarding the control of firewalls.

Verify the removal

If the removal wizard does not report a successful removal, but you think that it was successfully removed, verify the removal.

This situation can occur if you ran the removal wizard while the backup server was not running.

Steps

1) View the contents of the haStop.log log file generated by the removal wizard.

   a) In the **Control Center** tree of the **Control Center** icon, select **Logs**.

   b) Double-click **Server Logs**.

   c) Select the **High Availability Setup Wizard** node, then the **haStop.log** node.

   If you see information at the end of this log that indicates something other than the configuration completed, the removal wizard was not successful.

2) If removal wizard was not successful, you must troubleshoot this problem. Go back to the **Control Center** icon for the old backup server and try to run the **High Availability Removal Wizard** again. If it is not available to you (that is, you see the **High Availability Setup Wizard** node as opposed to the **High Availability Removal Wizard** node), you must contact Technical Support.

Completing the HA removal on a standalone Management Server or on one or two Management Servers of an HA pair

After you have successfully run the **High Availability Removal Wizard**, there are several additional steps to complete, depending on the way in which you want to control the firewalls for those Management Servers.

Keep firewalls with the former primary server

You can keep management control of all the firewalls with the former *primary* server.

Steps

1) Use the Control Center Client application to log on to the former primary server.

2) Apply the configuration to all the firewalls.

Keep firewalls with the former backup server

You can keep management control of all the firewalls with the former *backup* server.

Steps

1) Use the Control Center Client application to log on to the former backup server.

2) In the navigation bar, select **Maintenance**.

3) In the **Firewall Maintenance** tree, double-click **Device Control**. The **Device Control** window is displayed.

4) Select all the firewalls in the **Select Firewalls to control** list. In the **Control Actions** list, select **Request management control**.

5) Apply the configuration to all the firewalls.

Split firewalls between the two servers

You can *split* management control of the firewalls between the two servers.

Steps

1) Use the Control Center Client application to log on to the former primary server.

2) Apply the configuration to those firewalls that are going to remain under the control of this server.

3) [Optional — Perform while you are still on the former primary server] Delete the firewalls that are no longer needed (that is, that are not going to be managed by this Management Server).

4) Use the Control Center Client application to log on to the former backup server.

5) Open the **Device Control** window (by double-clicking **Device Control** in the **Firewall Maintenance** tree of the **Maintenance** icon).

6) Select all the firewalls and then select **Request management control**. Only those firewalls that were not applied to in Step 2 above will respond to this request.

7) Remaining on the former backup server, apply the configuration to all the firewalls. Again, only those firewalls that were not applied to in Step 2 will succeed.

8) [Optional] On the former backup server, delete the firewalls that are no longer needed (that will not be managed by this Management Server).

Related tasks

Restoring Management Servers that have failed completely on page 478

CHAPTER 43

Control Center audit

Contents

The Control Center has the ability to save, view, and archive specific actions that are performed by Control Center users on selected objects. The objects include, but are not limited to, firewalls, endpoints, services, access control rules, and alert processing rules.

About data management of Control Center audit

You can specify the audit trail data that is recorded by using the **Audit Trail Settings** window.

The resulting audit data can be viewed, filtered, and printed by using the **Audit Trail** page.

You can also export the Control Center audit data to one or more syslog servers by using the **Send Control Center Audit to Syslog Servers** window.

The auditing facility is not meant to maintain a full historical record of all of the tracked data. Instead, it is meant to provide a way to keep track of the user who performed specific actions on specific objects, and the time at which those actions occurred.

Although tracking specific changes made by Control Center users is a good practice, it can use a great deal of disk space. The audit data is stored in the audit tracking table in the Management Server database. This table grows without bounds and you should regularly archive or discard this data by using the options and features in the **Audit Trail Settings** window.

Note: Do not confuse the Control Center audit trail that provides a record of actions that are performed by Control Center users with security firewall-specific audit reports.

You can collect the information about specific actions that are performed on specific objects by Control Center users for a specific amount of time, and then you can store or purge the information.

All of the collected audit trail information is saved in tables in the Management Server database. You can configure the kind of data that is collected and the disposition of the data.

The audit information for the Control Center Client is stored in the path `<username>\AppData\Roaming\Forcepoint\Control Center`.

Note: In case the Client application hangs, the audit might not be deleted. You can manually delete the audit.

Related concepts

Managing firewall audit data on page 402

About Control Center audit

The auditing subsystem creates a chronological record of system events.

These records are used to:

- Reconstruct system events
- Deter improper system use
- Assign accountability for system activities
- Assess damage and allow efficient damage recovery
- Monitor problem areas of the system
- Produce reports and statistics about various system events

View audit trail information

The **Audit Trail** page is used to list, filter, preview, and print the audit trail data.

No previously-recorded information is changed when using this window. By default, all of the data is recorded until individual audit settings have been selected by using the **Audit Trail Settings** window.

You can use this data in a variety of ways. You can review activities that are performed by a specific user, track the specific activities that are performed on a specific firewall, or audit all of the activities that occurred in a specific time frame. These, and many other, audit trail filtering and presentation features are possible.

Steps

1) In the navigation bar, select **Control Center**.

2) Click the **Audit Trail** tab. The **Audit Trail** page is displayed.

3) Click **Settings** to configure specific actions for the identified objects.

4) Click **Filter** to specify a time range within which to view the audit data.

5) View details like object name, object change, ticket, raw and formatted data for the audit trail.

6) Click **Export** to save the file or print a report.

Configure a custom audit trail filter

Use the **Audit Trail Filter** window to configure a customized range of time that will be used to display the audit data on the **Audit Trail** page.

You can specify various types of ranges or milestones using the **Select time range** field.

Steps

1) If the **Audit Trail** page is already displayed, skip to Step 4.

2) In the navigation bar, click **Control Center**.

3) Click the **Audit Trail** tab. The **Audit Trail** page is displayed.

4) In the **Audit Trail** page, in the **Filter** list, select **Custom Time Range**. The **Audit Trail Filter** window is displayed.

5) From the **Select time range** options, select the custom time for the audit trail report. You can specify the conditional settings, start, and end time for the time range.

6) Click **OK**.

Manage audit trail information

The **Audit Trail Settings** window can be used to configure the audit data that is stored in the database of the Management Server.

The saved data can then be sorted (in ascending or descending order) by a specific column, and filtered by using existing column content or by using user-defined custom filters on one or more columns to provide precise control over the data that is presented in any view.

You can view or print the resulting data.

Steps

1) In the navigation bar, select **Control Center**.

2) Click the **Audit Trail** tab. The **Audit Trail** page is displayed.

3) Click **Settings**. The **Audit Trail Settings** window is displayed.

4) On the **Archive Settings** tab, select **Archive audit data** to enable archiving.

5) You can specify the number of days to keep the audit tracking data in the database. You can select **Purge archive data** to remove this data.

6) Select whether you want to archive data to a directory specified on the Management Server or a remote FTP server. Provide details for the FTP server.

7) Click **OK** to save these settings.

Export Control Center audit data using syslog

The Control Center generates its own audit data, which can include a variety of information.

- Log on
- Apply and validate
- Software updates
- Database updates

You can view this data on the **Audit Trail** page. However, you can also use syslog to send this data to event message collections, which are known as syslog servers or syslog daemons.

Syslog is a protocol that allows a machine to send event notification messages across IP networks to these event collectors. These messages are usually small and can be sent by using UPD or TCP.

Use the **Send Control Center Audit to Syslog Servers** window to configure the syslog server or servers to which the audit data will be sent.

Steps

1) In the navigation bar, select **Control Center**.
2) In the Control Center tree, expand the **Settings** node.
3) Double-click **Syslog**. The **Send Control Center Audit to Syslog Servers** window is displayed.
4) Select the **Enabled** check box to send audit data.
5) Enter the IP address and specify the **Remote Facility** to identify the audit export. The default value is local1.
6) In the **Advanced** options, configure more settings for the server.
7) Click **OK**.
   The syslog facility is now configured to export audit data.

Configure syslog server settings for a managed firewall

The **Syslog Server** window specifies the basic and advanced settings for the syslog server to which audit data is being sent from the firewall.

There are two slightly different versions of this window, depending on whether you are configuring it for firewall audit data or for Control Center audit data. The differences will be noted in the field descriptions.

Steps

1) In the navigation bar, select **Policy**.
2) In the lower left area of the window, click the **Firewall Settings** tab.
3) Double-click the **Firewall Syslog** node. The **Firewall Syslog** window is displayed.
4) In the **Export audit to syslog servers** table, click **Advanced** in the row of the syslog server for which you want to configure these additional settings. The **Syslog Server** window is displayed.

Configure syslog server settings for Control Center

The **Syslog Server** window specifies the basic and advanced settings for the syslog server to which audit data is being sent from the Control Center.

There are two slightly different versions of this window, depending on whether you are configuring it for firewall audit data or for Control Center audit data. The differences will be noted in the field descriptions.

Steps

1) In the navigation bar, select **Control Center**.
2) In the Control Center tree, expand the **Settings** node.
3) Double-click **Syslog**. The **Send Control Center Audit to Syslog Servers** window is displayed.
4) In the row of the syslog server for which you are configuring settings, click **Advanced**. The **Syslog Server** window is displayed.
5) In the **Basic Settings** area, specify details for the syslog server like server address and remote facility.
6) In the **Advanced Settings** area, specify details like server port, output data format, and message length.
7) Click **OK** to save these server settings.

Configure change tickets

Use the **Ticket** window to provide a name and description for the change ticket that you are starting.

When you start and stop a ticket, each of these actions will be represented in the audit data that is displayed on the **Audit Trail** page.

Steps

1) In the title bar, click (**Start Ticket**). The **Ticket** window is displayed.

   Note: You can stop the ticket by clicking the same icon in the title bar.

2) Specify a name for the ticket and provide a description.

   Note: For option descriptions, press **F1**.

3) Click **OK** to start the ticket. This starts tracking the audit data.

CHAPTER 44

Control Center updates and backup server status

Contents

Download, store, and manage the updates on the Control Center Management Server.

About Control Center Updates

Software updates include signed ePatch, hot fixes, and patches. An ePatch is an update that is provided directly by engineering to a specific customer. A hot fix is a customer-driven update to the Management Server software between updates.

Note: If your Control Center Management Servers are running in High Availability (HA) mode, you must first stop the High Availability servers, then install the updates to the Control Center Management Server, and then re-start the High Availability servers.

Updates are located at http://sidewinder.downloads.forcepoint.com. Update files can be downloaded directly to the Management Server by using **FTP**, **HTTP**, or **FILE** , or they can be downloaded to the Microsoft Windows platform on which the Control Center Client is installed and then uploaded to the Management Server. The **FILE** option loads a specific software update from a file already available on the Management Server.

Download and apply Management Server updates

Download and apply updates using the **Control Center Updates** page.

Steps

1) In the navigation bar, select **Control Center**.

2) Click the **Control Center Updates** tab. The **Control Center Updates** page is displayed.

3) On the **Upload to Server** tab, select and upload a file from the Client or a remote location to the Management Server. Alternatively, you can also select the **FILE** option to load the software update from a file already available on the Management Server at the specified location.

   A software update is uploaded to the Management Server.

4) On the **Uploaded Packages** tab, view the software updates that have been uploaded and select one of them and click **Apply**.

   The selected software update is applied to the Management Server.

File names for Control Center updates

Each type of Control Center update uses a different file naming convention.

Table 43: File names for Control Center updates

TAR file name	Update type	Example
[*release version* - 3 digits]	Patch	521.tar
[*release version* - 3 digits] [E] [*sequence number* - 2 digits]	ePatch	521E01.tar
[*release version* - 3 digits] [P] [*sequence number* - 2 digits]	Hot fix	521P01.tar

View the status of your backup Management Servers

To view the status of a backup Management Server, access the **Backup Server Status** page.

Steps

1) In the navigation bar, select **Control Center**.

2) Click the **Backup Server Status** tab. The **Backup Server Status** page is displayed.

   Note: This tab is available only if the Management Server is in HA mode.

3) View the node name, status, synchronization details of the backup Management Server.

Appendix A

Tips and troubleshooting

Contents

Use these basic solutions to troubleshoot issues with the Control Center Client application or the Control Center Management Server.

If you still have problems after trying these solutions, visit https://support.forcepoint.com.

Troubleshooting logging on

The following procedures are related to logon issues.

Logging on to the Management Server

If you experience problems logging on from the Client application computer to the Management Server, try the following solutions.

Are you using the correct user name and password?

You should be using the values that you specified during initial configuration for the **Control Center Admin (Client) Username** and **Control Center Admin Password** fields.

Can your Client computer resolve the host name of the Management Server?

From your Client computer, ping the host name of the Management Server. If the ping fails, add the host name to your name resolution system in either of these ways.

- If the Client computer is using a DNS server for name resolution, add the IP address and host name of the Management Server to the DNS server.
- Add the host name and IP address of the Management Server to the HOSTS file on your Client computer.
  1) Open the following file in Notepad: C:\WINDOWS\system32\drivers\etc\HOSTS

2) Add the Management Server IP address and host name to the file. The following is an example of the format to use:

```
1.2.3.4 host.example.com
```

3) Save the file.

Can the Client computer access required ports?

These ports are critical for communicating with the Management Server.

- Client to Management Server
  - **5432** — Management Server database
  - **9005** — Management Server HTTPS/SSL port
- HA server to HA server TCP ports
  - **22** — SSH
  - **5432** — Management Server database
  - **9005** — Management Server HTTPS/SSL port
- HA server to firewall TCP ports
  - **9005** — Management Server HTTPS/SSL port
- Firewall to HA server
  - **22** — SSH
  - **7080** — Management Server HTTP port
  - **9005** — Management Server HTTPS/SSL port
  - **9006** — utt_server (program for receiving Secure Alerts)

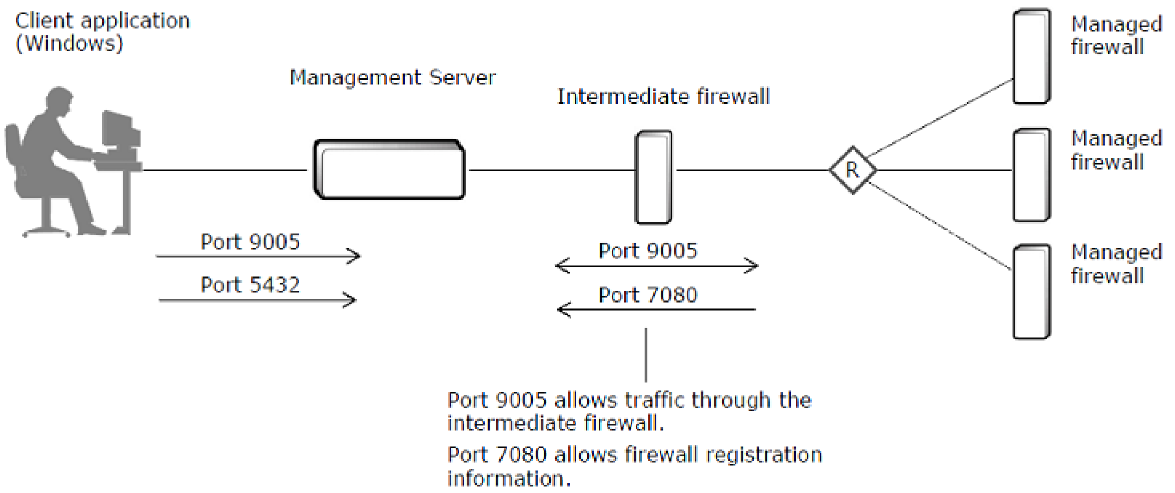
Do intermediate firewalls allow Control Center traffic?

If the Management Server is behind a firewall, the intermediate firewall must have an access control rule that allows Control Center traffic.

An intermediate firewall uses ports 9005 and 7080 for Control Center management. This creates a conflict when attempting to pass communication between a Management Server and managed firewalls. To allow Control Center traffic through the intermediate firewall, you must create a filter rule on ports 9005 and 7080.

- The filter rule must be created *before* you attempt to register the managed firewall appliances with the Management Server.
- The rule must be placed *above* the Control Center rule group

Figure 32: Management Server environment with an intermediate firewall



Communicating with a managed firewall

If you have problems communicating between the firewall and the Management Server, start by checking these common issues.

Are you using the host name of the Management Server?

Be sure to use the host name of the Management Server when you are registering a firewall. The Management Server name should match the host name of the Management Server that was specified when it was installed. The IP address of the Management Server can be specified as one of its interface IP addresses or as a NATed address, if necessary.

Verify Control Center management is enabled

Make sure Control Center management is enabled on the firewall.

Steps

1) Using the Forcepoint Sidewinder Admin Console, select **Maintenance** > **Control Center Registration**.

2) Verify the Management Server is registered.

3) Verify the Management Server names and IP addresses.

4) On the **Access Control Rules** window, verify that the Control Center access control rule group and its individual access control rules are enabled and correct.

Can the firewall access the required ports on the Management Server?

Make sure Management Server ports are configured correctly.

The following ports are critical for communicating with the Management Server.

- **7080** — This port is used to get the Management Server CA certificate from the Management Server to the firewall.
- **9005** — The Management Server listens on this port for secure (SSL) web service request/response traffic from the firewall. This port is also used for registration.

Change configuration parameters

You can reconfigure your Management Server.

Note: Performing this procedure resets the database to the default values.

Steps

1) Create a new ccinit.txt file and save it to a USB drive.

2) Log on to the console as `Administrative` user.

3) Change the user to `root`.

4) Run the following command:

```
touch /etc/sysconfig/gcc/setup/.configme
```

5) Insert the media with the new ccinit.txt file into the Management Server.

6) Restart the Management Server.

Troubleshooting network status using packet captures

Use packet captures to more closely evaluate attacks and network failures.

The packet capture session reveals information about trends, unexpected communications, and the absence of expected communications. The packet capture function accesses the TCP Dump tool on the firewall to perform the data capture session. You can also run sessions on several firewalls simultaneously.

How packet capture sessions can assist you

You can use packet capture sessions to gain valuable information when monitoring various traffic patterns.

The following examples demonstrate a few different ways that these sessions can be used.

Planned use

In this example, you prepare for future sessions by configuring all your sessions ahead of time.

1) Configure packet capture sessions in advance so that they are available as needed.
2) At a planned time, use the **Packet Capture** page to start and stop these sessions whenever you need them. Make sure to save the capture results before starting the session again. Otherwise, your results will be overwritten.
3) Save the results and view them.

As-needed use

In this example, you can configure your sessions as you need them.

1) A traffic pattern occurs that looks suspicious.
2) Configure your packet capture session now so that you can investigate this pattern.
3) Use the **Packet Capture** page to start and stop the session. Save the results, view them, and then delete them. (The deletion is optional. It is included in this example to show how temporary this process can be.)

Configure packet capture session criteria

You can configure a packet capture filter.

Steps

1) In the navigation bar, select **Monitor**.
2) Click the **Packet Capture** tab. The **Packet Capture** page is displayed.
3) Click **Add** or select a packet capture session and click **Edit**. The **Packet Capture Filter** window is displayed.

   Tip: For option descriptions, press **F1**.

4) Enter a name and description for the new filter.
5) [Optional] Select filter and port options.
6) Select the firewall, interfaces and zones to apply the filter to.

7) Click **OK**.

Result

The new packet capture filter is added to the list of filters on the **Packet Capture** page and can be selected when running packet captures.

Run packet capture sessions

You can run a packet capture session to check firewall network status.

Steps

1) In the navigation bar, select **Monitor**.

2) Click the **Packet Capture** tab. The **Packet Capture** page is displayed.

   Tip: For option descriptions, press **F1**.

3) Start the packet capture session.

   Tip: You can select multiple sessions. You can also run more than one session on the same firewall simultaneously.

4) Stop the session.

5) Click **Save as** to save the packet capture session to your local system.

Result

Use a third-party application, such as Wireshark® to view the packet capture data.

Troubleshooting connectivity to the Management Server

After you have configured the Control Center Management Server, you should ping the IP address of the Management Server from the Client application to verify connectivity.

If this ping fails:

1) Confirm that the network cable is plugged into the correct port on the Management Server.

2) Open the ccinit.txt file to confirm the IP address that you specified for the Management Server.

3) Confirm that the networking equipment connecting the Client application computer to the Management Server is configured correctly.

Report an issue

Use this procedure to report an issue while installing or using Control Center features.

Before you begin

Collate individual logs or have the support bundle ready.

For the beta release, report an issue.

Steps

1) Check for troubleshooting information in existing Control Center documents.
   - Product Guide
   - Quick Start Guide
   - Knowledge Base articles

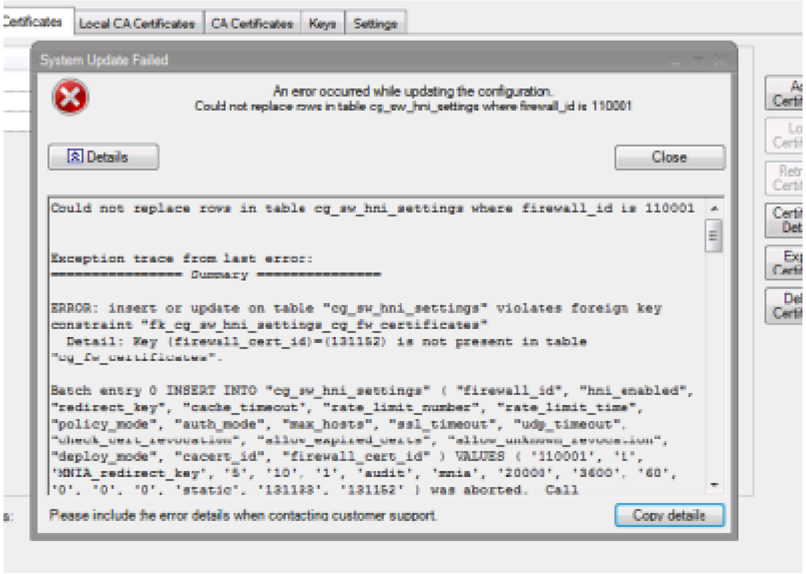
   Refer to the *Required documentation* section for helpful documents.

2) Send the logs or support bundle to Forcepoint support for resolution.

Obtain Control Center Client application logs

Save the Client application logs and send to Forcepoint support for resolution.

Figure 33: A sample client error



System Update Failed

An error occurred while updating the configuration.
Could not replace rows in table cg_sw_hni_settings where firewall_id is 110001

```
Could not replace rows in table cg_sw_hni_settings where firewall_id is 110001


Exception trace from last error:
================ Summary ================

ERROR: insert or update on table "cg_sw_hni_settings" violates foreign key
constraint "fk_cg_sw_hni_settings_cg_fw_certificates"
  Detail: Key (firewall_cert_id)=(131152) is not present in table
"cg_fw_certificates".

Batch entry 0 INSERT INTO "cg_sw_hni_settings" ( "firewall_id", "hni_enabled",
"redirect_key", "cache_timeout", "rate_limit_number", "rate_limit_time",
"policy_mode", "auth_mode", "max_hosts", "ssl_timeout", "udp_timeout",
"check_cert_revocation", "allow_expired_certs", "allow_unknown_revocation",
"deploy_mode", "cacert_id", "firewall_cert_id" ) VALUES ( '110001', '1',
'MNIA_redirect_key', '5', '10', '1', 'audit', 'mnia', '20000', '3600', '60',
'0', '0', '0', 'static', '131133', '131152' ) was aborted.  Call
```

Please include the error details when contacting customer support.

Steps

1) Make a note of the steps that you performed prior to getting a client error.

2) View the error window and details.

3) Click **Copy Details**.

4) The log files are saved in the default location `C:\Users\<username>\AppData\Roaming\r\Control Center\logs`.

Result

Send the logs to Forcepoint support for resolution.

Obtain support bundle for Control Center Management Server

Create a support bundle using the Client application. This is a consolidated file of all the logs from the Control Center server.

Steps

1) In the navigation bar, select **Control Center**.

2) In the Control Center tree, double-click the **Support Tool** node.

   The **Support Tool** window is displayed.

3) Enter a service request number.

4) (Optional) Select the **Include database backup** check box if you want to include the database information in the support bundle.

5) Click **Create Support File**.

   The server support bundle is created in the default path `/var/cc/support/SR_<Service Request number>` This is a .tar.gz file.

6) Click **Export** to save this on your local system.

Result

Send the support bundle to Forcepoint support for resolution.

Appendix B

Glossary

A	
access control rule	A rule that provides the network security mechanism to control the flow of data into and out of the internal network.
application	An object that identifies the network application that is associated with a connection.
Application Defense	An object that is used to refine access control rules for specific applications and to configure key services such as virus protection, spyware protection, and web services management.
Application Defense group	An object that contains one or more Application Defense objects. An Application Defense group is used in access control rules to specify advanced application policy.
application discovery	A process of identifying the applications that are allowed to be used in a zone.
authentication	A process that validates a person's identity before he or she is allowed to log on to the Control Center Management Server or to pass traffic through a firewall.
B	
burb	[For firewall version 7.x only] A type-enforced network area that is used to isolate network interfaces from each other. These areas are treated the same from the point of view of security policy for a system. For version 8.0.0 or later firewalls, the term *zone* is used instead of burb.
C	
client	A program or a user who requests one or more network services from a server.
Client application	An application that resides on a desktop computer that is running a Windows operating system. The application provides the user interface to configure, manage, and monitor supported firewalls, and to perform Control Center administrative tasks.
D	
device group	A collection of one or more firewalls that can be managed as a group.
domain	(1) In reference to networking, the portion of an Internet address that indicates the name of a computer network. For example, in the jones@example.sales.com e-mail address, the domain is example.sales.com. (2) In reference to Type Enforcement, an attribute that is applied to a process that is running on SecureOS that determines the system operation that the process can perform.
Domain Name System (DNS)	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 than a 32-bit internet address.
E	
external DNS	A system that 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 of a firewall.
F	

failover	See *High Availability*.
firewall	The term used for the Forcepoint Sidewinder.
H	
High Availability (HA)	A feature that refers to two Control Center Management Servers that are configured to work together to provide redundancy and continuity.
host	Any computer that is connected to a network, such as a workstation, router, firewall, or server.
I	
identity validation	A process that is used to establish the identity of a user who is attempting to access a firewall.
inbound connection	A connection that passes from the Internet zone to the protected zone.
IPv4 address	A 32-bit address that is 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 that is associated with the growth of the number of computers that are attached to the Internet.
L	
link aggregation	A process that is used to bundle multiple NICs into a group. There are two different types of NIC groups that are available for configuration: • **Aggregate** — [Available only for version 8.0.0 or later firewalls] Provides increased bandwidth • **Redundant** — Used for failover purposes
M	
Management Server	A hardened Linux platform that provides the firewall management and monitoring capabilities that are required to centrally manage security policy.
N	
NAT (network address translation)	Changing the source address of a packet to a new IP address that is specified by the administrator.
net mask	The way that computers know the part of a TCP/IP address that refers to the network, and the part that 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, and so on).
O	
outbound connection	A connection that passes from the 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, and so on.)

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 widely used.
proxy	A software agent that acts on behalf of a user who is requesting a network connection through the firewall. A proxy accepts a connection from a user, makes a decision as to whether the user or client IP address is permitted to use the proxy, optionally performs additional authentication, and then completes a connection, on behalf of the user, to a remote destination.
Q	
R	
redundant	See *link aggregation*.
remote certificate	Identification for one or more peers that can be involved in a VPN connection with a firewall. This is also the certificate that the Control Center will use for its TLS/SSL connection to the McAfee Logon Collector. This certificate identifies the Control Center Management Server to the McAfee Logon Collector server.
S	
server	A computer system that provides services (such as FTP) to a network. It can also refer to a program that is 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.
Simple Mail Transport Protocol)	(SMTP) The TCP/IP protocol that transfers email as it moves through the system.
SSH content inspection	A process that decrypts SSH connections, inspects content, and then re-encrypts the traffic before it is sent to its destination.
SSL content inspection	A process that decrypts HTTPS and SSL connections, inspects them, and then re-encrypts them if requested. SSL rules determine the way that the firewall processes encrypted SSL connections that match an access control rule. By default, SSL connections are not decrypted.
SSL rule	A rule that 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	
Type Enforcement	A security technology that was developed to protect against intruders by preventing someone from taking over the UNIX operating system within a firewall and accessing critical files or doing other damage.
U	
USB drive	A portable flash memory card that plugs into the USB port of a computer.
Z	
zone	[For firewalls version 8.0.0 or later] A type-enforced network area that is used to isolate network interfaces from each other. These areas are treated the same from the point of view of security policy for a system. For version 7.x firewalls, the term *burb* is used instead of zone.

Index