Next Generation Firewall

6.9

Installation Guide

Revision A

Published 08 December 2020

Contents

Preface

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

Conventions

The following typographical conventions and icons are used.

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.

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, release notes, Knowledge Base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint support website. If you do not yet have credentials, create a customer account. See https://support.forcepoint.com/CreateAccount.

Part I

Introduction to the Forcepoint Next Generation Firewall solution

Contents

Before setting up Forcepoint Next Generation Firewall (Forcepoint NGFW), it is useful to know what the different components do and what engine roles are available. There are also tasks that you must complete to prepare for installation.

Chapter 1

Introduction to Forcepoint NGFW

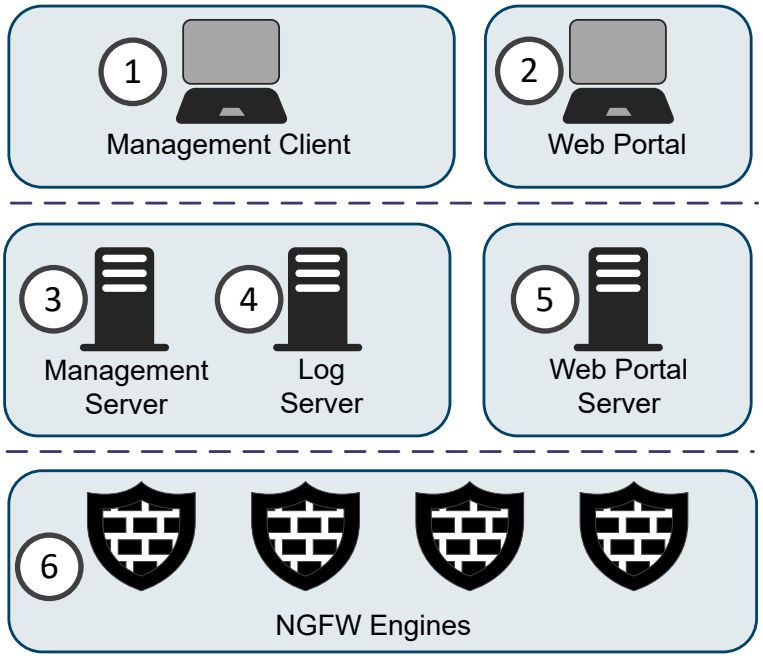
Contents

The Forcepoint Next Generation Firewall solution consists of Forcepoint NGFW Engines and the Forcepoint NGFW Security Management Center (SMC). The SMC is the management component of the Forcepoint NGFW solution.

Components in the Forcepoint NGFW solution

The Forcepoint NGFW solution includes NGFW Engines, SMC server components, and SMC user interface components.

Components in the Forcepoint NGFW solution



1. The Management Client is the user interface for the SMC that you use for all configuration and monitoring tasks. You can have an unlimited number of Management Clients.
2. The Web Portal is the browser-based user interface for the services provided by the Web Portal Server.
3. The Management Server is the central component for system administration. One Management Server can manage many different types of NGFW Engines.
4. The Log Server stores traffic logs that can be managed and compiled into reports. Log Servers also correlate events, monitor the status of NGFW Engines, show real-time statistics, and forward logs to third-party devices.
5. The Web Portal Server is a separately licensed optional component that provides restricted access to log data, reports, and policy snapshots.
6. NGFW Engines inspect traffic. You can use NGFW Engines in the Firewall/VPN, IPS, or Layer 2 Firewall role.

Security Management Center

The basic SMC components are the Management Server, Log Server, and one or more Management Clients.

The Management Client is the user interface for the SMC. You can use the same SMC installation to manage multiple NGFW Engines in different roles.

The SMC can optionally include multiple Management Servers, multiple Log Servers, and multiple Web Portal Servers. Your licenses specify the type and number of optional components and engines that your environment can include. You can install the SMC components separately on different computers or on the same computer, depending on your performance requirements. The SMC all-in-one appliance is shipped with the Management Server and a Log Server pre-installed on it.

NGFW Engines

You can use NGFW Engines in the Firewall/VPN, IPS, and Layer 2 Firewall roles. You can also use NGFW Engines as Master NGFW Engines to host Virtual NGFW Engines in these roles.

NGFW Engines are represented by different types of NGFW Engine elements in the SMC. The following elements represent NGFW Engines in the SMC:

Engine Role	Elements
Firewall/VPN	**Single Firewall** elements represent firewalls that consist of one physical device. **Firewall Cluster** elements consist of 2–16 physical firewall devices that work together as a single entity. **Virtual Firewall** elements are Virtual NGFW Engines in the Firewall/VPN role.
IPS	**Single IPS** elements represent IPS engines that consist of one physical IPS device. **IPS Cluster** elements combine 2–16 physical IPS devices into a single entity. **Virtual IPS** elements are Virtual NGFW Engines in the IPS role.
Layer 2 Firewall	**Single Layer 2 Firewall** elements represent Layer 2 Firewalls that consist of one physical device. **Layer 2 Firewall Cluster** elements combine 2–16 physical Layer 2 Firewall devices into a single entity. **Virtual Layer 2 Firewall** elements are Virtual NGFW Engines in the Layer 2 Firewall role.
Master NGFW Engine	**Master NGFW Engine** elements represent physical devices that host Virtual NGFW Engines.

These elements are containers for the main configuration information directly related to the NGFW Engines.

Forcepoint NGFW in the Firewall/VPN role

In addition to standard firewall features, Forcepoint NGFW in the Firewall/VPN role provides several advanced features.

The main features of Forcepoint NGFW in the Firewall/VPN role include:

- **Advanced traffic inspection** — Multi-Layer packet and connection verification process provides maximum security without compromising system throughput. An anti-malware scanner and web filtering complement the standard traffic inspection features when the firewall is licensed for the UTM (unified threat management) feature. Anti-malware is not supported on Virtual Firewalls. Master NGFW Engines do not directly inspect traffic.
- **Built-in load balancing and high availability** — The clustering of the firewall nodes is integrated. The firewall dynamically load-balances individual connections between the cluster nodes.
- **Multi-Link technology** — Multi-Link allows configuring redundant network connections without the more complex traditional solutions that require redundant external routers and switches. It provides high availability for inbound, outbound, and VPN connections.
- **QoS and bandwidth management** — You can set up the minimum and maximum bandwidth value and the priority value for different types of traffic.
- **Virtual private networks** — The firewall provides fast, secure, and reliable VPN connections with the added benefits of the clustering and Multi-Link technologies. These features provide load balancing and failover between ISPs and VPN gateways.
- **Unified SMC and integration with other NGFW Engines** — You can configure and monitor the Firewall/VPN and the other NGFW Engines through the same SMC and the same user interface. The SMC provides extensive reporting tools for generating statistical reports based on logs, alerts, and operating statistics.

Forcepoint NGFW in the IPS and Layer 2 Firewall roles

IPS engines and Layer 2 Firewalls pick up network traffic, inspect it, and create event data for further processing by the Log Server.

The main features of Forcepoint NGFW in the IPS and Layer 2 Firewall roles include:

- **Multiple detection methods** — Misuse detection uses fingerprints to detect known attacks. Anomaly detection uses traffic statistics to detect unusual network behavior. Protocol validation identifies violations of the defined protocol for a particular type of traffic. Event correlation processes event information to detect a pattern of events that might indicate an intrusion attempt.
- **Response mechanisms** — There are several response mechanisms to anomalous traffic. These include different alerting channels, traffic recording, TCP connection termination, traffic blacklisting, and traffic blocking with Inline Interfaces.
- **Unified SMC and integration with other NGFW Engines** — The IPS engines, Layer 2 Firewalls, Master NGFW Engines, Virtual IPS engines, and Virtual Layer 2 Firewalls are managed centrally through the SMC. The SMC provides extensive reporting tools for generating statistical reports based on logs, alerts, and operating statistics.

Master NGFW Engines and Virtual NGFW Engines

Master NGFW Engines are physical devices that provide resources for multiple Virtual NGFW Engines.

Any NGFW Engine that has a license that allows the creation of Virtual Resources can be used as a Master NGFW Engine. Virtual NGFW Engines are represented by the following elements in the SMC:

- *Virtual Firewall* is a Virtual NGFW Engine in the Firewall/VPN role.
- *Virtual IPS engine* is a Virtual NGFW Engine in the IPS role.

- *Virtual Layer 2 Firewall* is a Virtual NGFW Engine in the Layer 2 Firewall role.

Each Master NGFW Engine can only host one Virtual NGFW Engine role. To use more than one Virtual NGFW Engine role, you must create a separate Master NGFW Engine for each Virtual NGFW Engine role. Each Master NGFW Engine must be on a separate physical Master NGFW Engine device.

Chapter 2

Preparing for installation

Contents

Before installing Forcepoint NGFW, identify the components of your installation and how they integrate into your environment.

Supported platforms

Several platforms are supported for deploying Forcepoint NGFW and SMC components.

CAUTION

To protect the privacy of your data, we recommend using dedicated hardware for all NGFW, SMC, and SMC Appliance installations. For cloud-based virtualization platforms, use an instance type that runs on dedicated hardware. For on-premises virtualization platforms, install the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines. For third-party hardware, do not install any other software on the computer where you install the NGFW Engines or SMC components.

Supported platforms for SMC deployment

SMC server components can be installed on third-party hardware or they are available as a dedicated Forcepoint NGFW Security Management Center Appliance (SMC Appliance).

Third-party hardware

CAUTION

Do not install the SMC components on Forcepoint NGFW hardware.

- You can install the SMC on third-party hardware that meets the hardware requirements. For information about hardware requirements, see the Release Notes.
- You can install all SMC server components on the same computer, or install separate components on different computers.
- In a large or geographically distributed deployment, we recommend installing the Management Server, Log Server, and optional Web Portal Server on separate computers.

SMC Appliance

The Management Server and a Log Server are integrated with the hardware operating system as a dedicated server appliance.

Supported platforms for Forcepoint NGFW deployment

You can run NGFW Engines on various platforms.

The following general types of platforms are available for NGFW Engines:

- Purpose-built Forcepoint NGFW appliances

  Note

  For information about supported appliance models, see Knowledge Base article 9743.

- VMware ESX and KVM virtualization platforms
- Microsoft Hyper-V virtualization platform (Firewall/VPN role only)
- Microsoft Azure cloud (Firewall/VPN role only)
- Amazon Web Services (AWS) cloud (Firewall/VPN role only)
- Third-party hardware that meets the hardware requirements

For supported versions of virtualization platforms, see the Release Notes.

The NGFW Engine software includes an integrated, hardened Linux operating system. The operating system eliminates the need for separate installation, configuration, and patching.

Deploying NGFW Engines on cloud-based virtualization platforms

You can deploy NGFW Engines on cloud-based virtualization platforms, such as the Amazon Web Services (AWS) cloud and the Microsoft Azure cloud.

NGFW Engines on cloud-based virtualization platforms provide VPN connectivity, access control, and inspection for services hosted on cloud-based virtualization platforms.

For information about deploying NGFW Engines in the AWS cloud, see the document *How to deploy Next Generation Firewall in the Amazon Web Services cloud* and Knowledge Base article 10156.

For information about deploying NGFW Engines in the Azure cloud, see the document *How to deploy Next Generation Firewall in the Azure cloud* and Knowledge Base article 14485.

After deployment, you can manage NGFW Engines on cloud-based virtualization platforms using the Management Client in the same way as other NGFW Engines. If you deploy NGFW Engines that use the scaling feature, you can only preview the NGFW Engines and make changes to the Firewall policies.

Note

Only the Firewall/VPN role is supported. Firewall Clusters, Master NGFW Engines, and Virtual Firewalls are not supported.

Licensing

Two licensing models are supported.

- **Bring Your Own License** — You pay only the AWS or Azure standard runtime fee for the NGFW Engine instance. You must install a license for the NGFW Engine in the SMC.
- **Hourly** (pay as you go license) — You pay the AWS or Azure standard runtime fee for the NGFW Engine instance plus an hourly license fee based on the runtime of the NGFW Engine. No license installation is needed for the NGFW Engine in the SMC.

For features that require separate licenses, the SMC automatically detects which licensing model the NGFW Engine uses.

Support for scaling in cloud-based virtualization platforms

When NGFW Engines are deployed from the Microsoft Azure or AWS cloud environment, additional instances can be created and removed, depending on traffic load.

You deploy the Cloud Auto-Scaled Firewalls from the cloud environment, and in the Management Client, the Cloud Auto-Scaled Firewalls are automatically added to Cloud Auto-Scaled Group elements. You can monitor the Cloud Auto-Scaled Firewalls in the Home View, for example.

Limitations

- Cloud Auto-Scaled Firewalls cannot be edited in the Management Client.
- The automatic scaling feature is only supported in the Azure cloud. In the AWS cloud, you must add and remove instances manually.

Running NGFW Engines as Master NGFW Engines

There are some hardware requirements and configuration limitations when you use an NGFW Engine as a Master NGFW Engine.

Running the NGFW Engine as a Master NGFW Engine does not require a third-party virtualization platform. When you run Forcepoint NGFW as a Master NGFW Engine, the Forcepoint NGFW hardware provides the virtual environment and resources for the hosted Virtual NGFW Engines. You must always install the Forcepoint NGFW software on a hardware device to run the NGFW Engine as a Master NGFW Engine.

You can run Master NGFW Engines on the following types of hardware platforms:

- Purpose-built Forcepoint NGFW appliances with 64-bit architecture
- Third-party hardware with 64-bit architecture that meets the hardware requirements

For information about system requirements, see the Release Notes.

The following limitations apply when you use an NGFW Engine as a Master NGFW Engine:

- Each Master NGFW Engine must run on a separate 64-bit physical device.
- All Virtual NGFW Engines hosted by a Master NGFW Engine or Master NGFW Engine cluster must have the same role and the same Failure Mode (*fail-open* or *fail-close*).
- Master NGFW Engines can allocate VLANs or interfaces to Virtual NGFW Engines. If the Failure Mode of the Virtual IPS engines or Virtual Layer 2 Firewalls is *Normal* (fail-close) and you want to allocate VLANs to several engines, you must use the Master NGFW Engine cluster in standby mode.

Clustering

There are special considerations when you deploy an NGFW Engine as a Firewall Cluster, IPS Cluster, or Layer 2 Firewall Cluster.

Heartbeat connection and state synchronization for clusters

The nodes in a cluster use a heartbeat connection to monitor the other nodes' operation and to synchronize their state tables.

The nodes in a cluster exchange status information through a heartbeat network using multicast transmissions. If a node becomes unavailable, the other nodes of the cluster immediately notice the change, and connections are reallocated to the available nodes. A dedicated network is recommended for at least the primary heartbeat communications.

The heartbeat connection is essential for the operation of the cluster. Make sure that these conditions are true:

- The heartbeat network works correctly and reliably.
- You are using the correct type of network cables (after testing that they work).
- The network interface cards' duplex and speed settings match.
- Any network devices between the nodes are correctly configured.

It is possible to authenticate and encrypt the heartbeat traffic.

Problems in the heartbeat network might seriously degrade the performance and operation of the cluster.

In the Firewall/VPN role, the nodes of a Firewall Cluster periodically exchange synchronization messages to synchronize state data.

Hardware for Firewall Cluster nodes

You can run different nodes of the same cluster on different types of hardware.

The hardware the cluster nodes run on does not need to be identical. Different types of equipment can be used as long as all nodes have enough network interfaces for your configuration. Firewall Clusters can run on a

Forcepoint NGFW appliance, on a standard server with an Intel-compatible processor, or as a virtual machine on a virtualization platform.

If equipment with different performance characteristics is clustered together, the load-balancing technology automatically distributes the load so that lower performance nodes handle less traffic than the higher performance nodes. However, when a node goes offline, the remaining nodes must be able to handle all traffic on their own to ensure high availability. For this reason, it is usually best to cluster nodes with similar performance characteristics.

Deployment options for Forcepoint NGFW Engines

There are several ways to deploy Forcepoint NGFW Engines depending on how you want to inspect and respond to traffic.

Deployment options for Forcepoint NGFW

Forcepoint NGFW role	Deployment type	Description
Firewall/VPN	Layer 3 deployment only	NGFW Engines in the Firewall/VPN role have only Layer 3 Physical Interfaces. The NGFW Engines provide only the features and traffic inspection that are available for NGFW Engines in the Firewall/VPN role.
	Multi-layer deployment	NGFW Engines in the Firewall/VPN role have both Layer 2 Physical Interfaces and Layer 3 Physical Interfaces. Layer 2 Physical Interfaces on NGFW Engines in the Firewall/VPN role allow the engine to provide the same kind of traffic inspection that is available for NGFW Engines in the IPS and Layer 2 Firewall roles. The NGFW Engine also supports the features and traffic inspection that are available for NGFW Engines in the Firewall/VPN role. **Note** Multi-layer deployment requires advanced configuration that is outside the scope of this guide. For configuration steps, see the *Forcepoint Next Generation Firewall Product Guide*.
IPS	Inline	The traffic flows through the IPS engine. The IPS engine has full control over the traffic flow and can automatically block any traffic. An inline IPS engine can also enforce blacklisting commands from other components. Fail-open network cards can ensure that traffic flow is not disrupted when the IPS engine is offline. An inline IPS engine also provides access control and logging for any Ethernet traffic (layer 2).
	Capture	External equipment duplicates the traffic flow for inspection, and the IPS engine passively monitors traffic. The IPS engine does not have direct control over the traffic flow, but it can respond to selected threats by sending packets that reset the connections. An IDS-only IPS engine can send blacklisting requests to other IPS engines, Layer 2 Firewalls, or Firewalls, but it cannot enforce blacklisting requests from other components.

Forcepoint NGFW role	Deployment type	Description
Layer 2 Firewall	Inline	The traffic flows through the Layer 2 Firewall. The Layer 2 Firewall has full control over the traffic flow and can automatically block any traffic. An inline Layer 2 Firewall can also enforce blacklisting commands received from other components. An inline Layer 2 Firewall also provides access control and logging for any Ethernet traffic (layer 2).
	Capture (Passive Firewall)	In a Capture (Passive Firewall) installation, external equipment duplicates the traffic flow for inspection to the Layer 2 Firewall, and the Layer 2 Firewall passively monitors traffic. The Layer 2 Firewall does not have direct control over the traffic flow, but it can respond to selected threats by sending packets that reset the connections. A Layer 2 Firewall in Passive Firewall mode can send blacklisting requests to other Layer 2 Firewalls, IPS engines, or Firewalls. It cannot enforce blacklisting requests from other components.
	Passive Inline	In a Passive Inline installation, the traffic flows through the Layer 2 Firewall, but the Layer 2 Firewall only logs connections. A Layer 2 Firewall in Passive inline mode can send blacklisting requests to other Layer 2 Firewalls, IPS engines, or Firewalls. It cannot enforce blacklisting requests from other components.

There are two ways to connect Capture Interfaces on Firewalls, IPS engines, and Layer 2 Firewalls to your networks to capture network traffic.

Network connection options for Capture Interfaces

Option	Description
Switched Port Analyzer (SPAN) port	A SPAN port captures network traffic to a defined port on an external switch. This action is also known as port mirroring. The capturing is passive, so it does not interfere with the traffic. All traffic to be monitored must be copied to this SPAN port.
Network Test Access Port (TAP)	A network TAP is a passive device at the network wire between network devices. The capturing is done passively, so it does not interfere with the traffic. With a network TAP, the two directions of the network traffic are divided to separate wires. For this reason, the IPS engine or Layer 2 Firewall needs two capture interfaces for a network TAP; one capture interface for each direction of the traffic. The two related capture interfaces must have the same logical interface that combines the traffic of these two interfaces for inspection. You could also use the pair of capture interfaces to monitor traffic in two separate network devices.

Cable connection guidelines

Follow these cable connection guidelines when connecting cables to Forcepoint NGFW hardware and the SMC Appliance.

Cable connection guidelines for SMC Appliance

For an SMC Appliance, make sure that all copper cables are correctly rated (CAT 5e or CAT 6 in gigabit networks).

Cable connection guidelines for Firewalls

The cabling of Firewalls depends on the engine type and the installation.

Make sure that all Ethernet cables are correctly rated (CAT 5e or CAT 6 in gigabit networks).

If you have a two-node Firewall Cluster, it is recommended to use a crossover cable without any intermediary devices between the nodes. If you use an external switch between the nodes, follow these guidelines:

- Make sure that portfast is enabled on the external switches.
- Make sure that the speed/duplex settings of the external switches and the Firewall devices are set to Auto.
- Configure the external switches to forward multicast traffic.

For layer 2 physical interfaces on Firewalls, follow these cable connection guidelines:

- Capture interfaces — Follow the cable connection guidelines for IPS and Layer 2 Firewalls.
- Inline IPS interfaces — Follow the cable connection guidelines for IPS.
- Inline Layer 2 Firewall interfaces — Follow the cable connection guidelines for Layer 2 Firewalls.

Cable connection guidelines for IPS and Layer 2 Firewalls

The cabling of IPS engines and Layer 2 Firewalls depends on the engine type and the installation.

Make sure that all Ethernet cables are correctly rated (CAT 5e or CAT 6 in gigabit networks).

Follow standard cable connections with inline IPS engines and Layer 2 Firewalls:

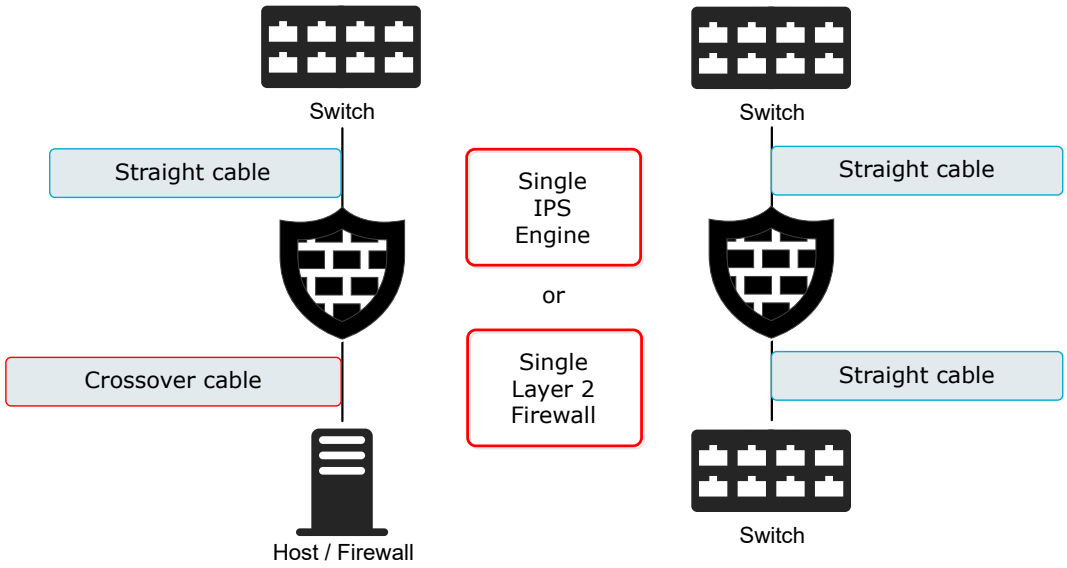
- Use straight cables to connect the IPS engines and Layer 2 Firewalls to external switches.
- Use crossover cables to connect the IPS engines and Layer 2 Firewalls to hosts (such as routers or Firewalls).

Note

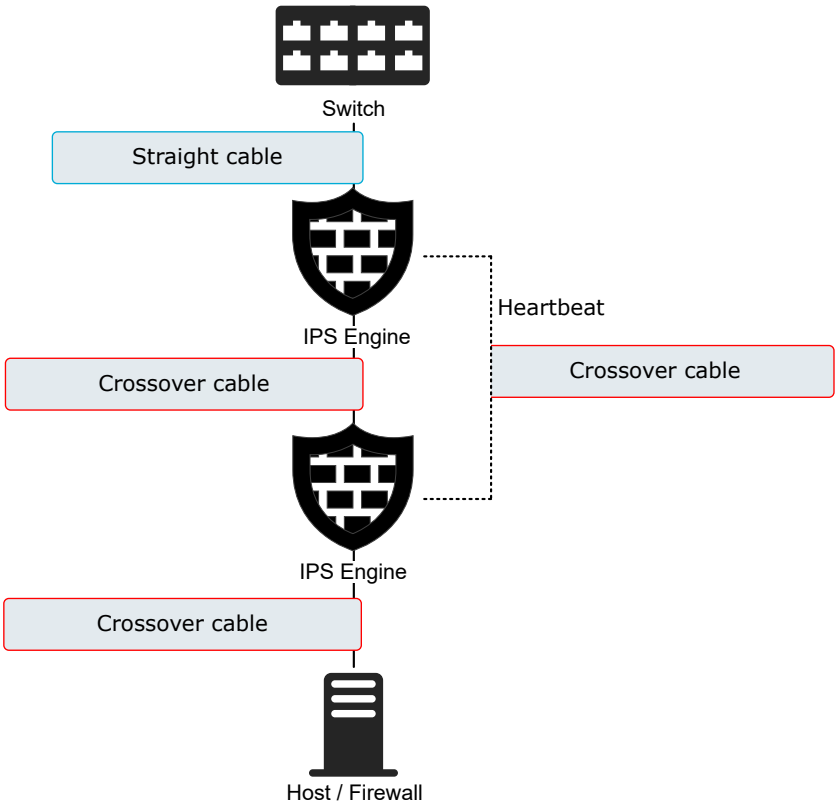
Fail-open network interface cards support Auto-MDIX, so both crossover and straight cables might work when the IPS engine is online. However, only the correct type of cable allows traffic to flow when the IPS engine is offline and the fail-open network interface card is in bypass state. It is recommended to test the IPS deployment in offline state to make sure that the correct cables are used.

Cable connections for Master NGFW Engines that host Virtual IPS engines or Virtual Layer 2 Firewalls follow the same principles as the connections for inline IPS engines and Layer 2 Firewalls.

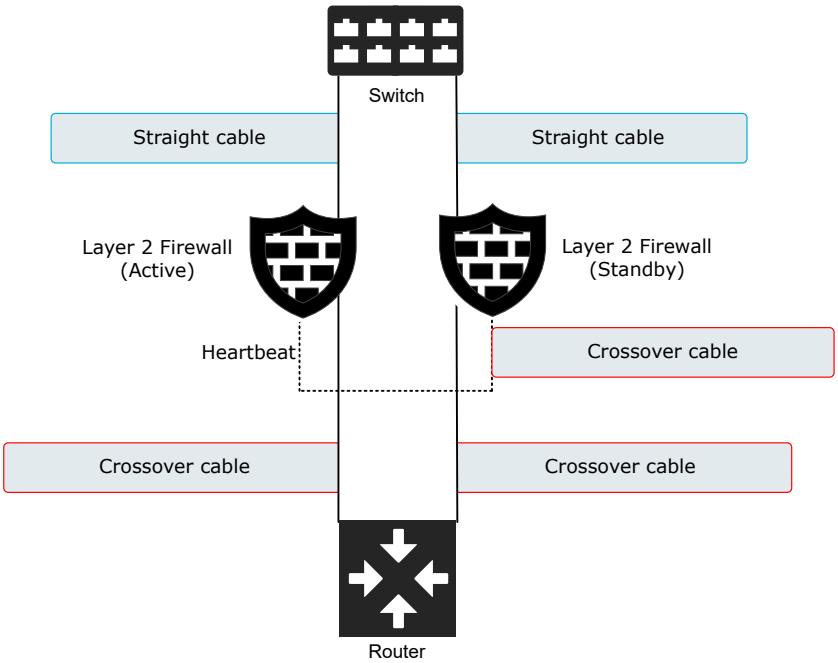
Correct cable types for Single IPS engines and Single Layer 2 Firewalls



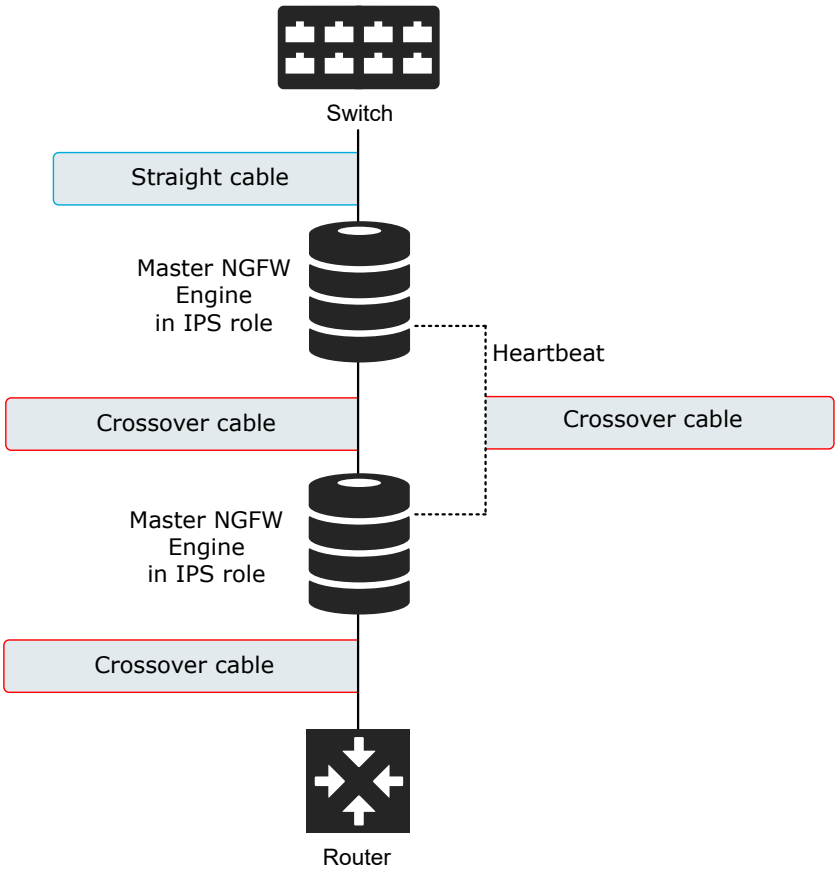
Correct cable types for Serial IPS Clusters



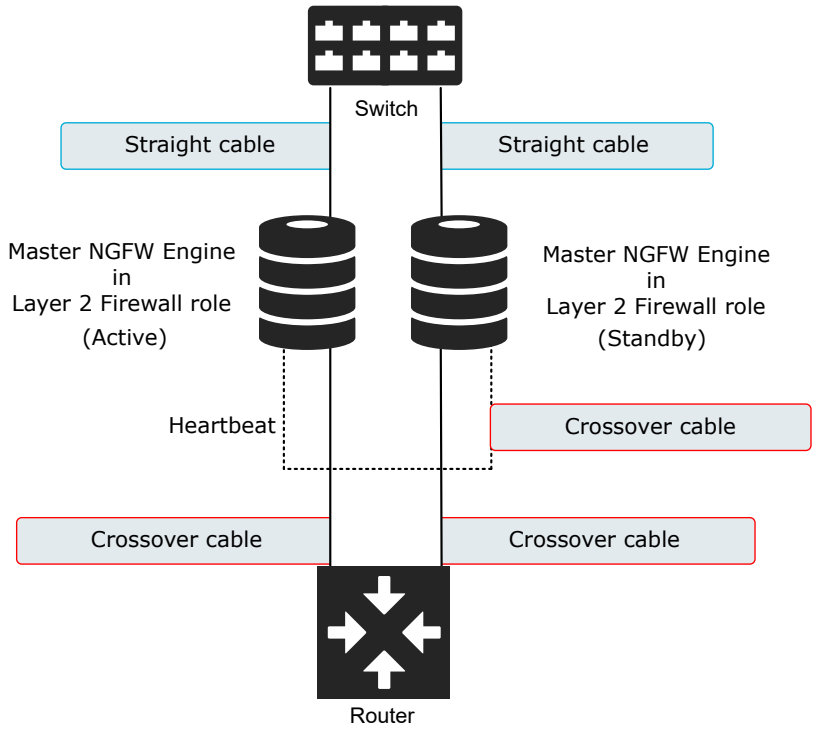
Correct cable types for Active/Standby Layer 2 Firewall Clusters



Correct cable types for Serial Virtual IPS Clusters



Correct cable types for Active/Standby Virtual Layer 2 Firewall Clusters



Speed and duplex settings for NGFW Engines

Mismatched speed and duplex settings are a frequent source of networking problems.

The basic principle for speed and duplex settings is that network cards at both ends of each cable must have identical settings. This principle also applies to the automatic negotiation setting: if one end of the cable is set to auto-negotiate, the other end must also be set to auto-negotiate and not to any fixed setting. Gigabit standards require interfaces to use auto-negotiation. Fixed settings are not allowed at gigabit speeds.

For Inline Interfaces, the settings must be identical on both links within each Inline Interface pair. Use identical settings on all four interfaces, instead of just matching settings at both ends of each cable (two + two interfaces). If one of the links has a lower maximum speed than the other link, the higher-speed link must be set to use the lower speed.

Obtain installation files

If you did not receive an installation DVD for the Forcepoint NGFW software or the SMC, download installation files.

You do not have to download installation files under these circumstances:

- Forcepoint NGFW appliances and the SMC Appliance are delivered with the necessary software pre-installed on them. You do not need to download installation files for these appliances.

- You might have received ready-made installation DVDs of the Forcepoint NGFW software and the SMC software.

Download installation files

Download the files you need to install the Forcepoint NGFW software and the SMC components.

Installation files for the SMC components are available only as .zip files. Installation files for the Forcepoint NGFW software are available as .zip files or .iso image files.

Steps

1) Go to https://support.forcepoint.com.
2) Log on using an existing user account.
3) Select **Downloads**.
4) Under **Network Security**, click the version of the SMC software that you want to download, then download the .zip file installation file.
5) Under **Network Security**, click the version of the Forcepoint NGFW software that you want to download, then select the type of installation file to download.
   - The .zip file is used in the remote upgrade on all supported platforms. It can also be used for a local upgrade from a USB drive or a non-bootable DVD.
   - The .iso file allows you to create a bootable installation DVD for a local upgrade on platforms that have an optical drive.

Check file integrity

Before installing the Forcepoint NGFW software from downloaded files, check that the installation files have not become corrupt or been changed.

Using corrupt files might cause problems at any stage of the installation and use of the system. Check file integrity by generating a file checksum of the files. Compare the checksum of the downloaded files with the checksum for the software version in the Release Notes or on the download page at the Forcepoint website.

Note

In Windows environments, you can use Windows PowerShell to generate checksums. Several third-party programs are also available.

Steps

1) Look up the correct checksum at https://support.forcepoint.com.
2) Change to the directory that contains the files to be checked.
3) Generate a checksum of the file using one of the following commands, where `filename` is the name of the installation file:

- `sha1sum filename`
- `sha256sum filename`
- `sha512sum filename`

4) Compare the displayed output to the checksum for the software version. They must match.

CAUTION

Do not use files that have invalid checksums. If downloading the files again does not help, contact Forcepoint support to resolve the issue.

Next steps

If you downloaded the installation files as a .zip file, unzip the contents at the installation location and install the licenses.

Create an installation DVD for Forcepoint NGFW software

To use the installation DVD successfully, it must have the correct structure stored in the .iso images. Otherwise you cannot use it for installing the Forcepoint NGFW software.

Steps

1) Use a DVD burning application that can correctly read and burn the DVD structure stored in the .iso image for the Forcepoint NGFW software.

   For instructions, see the documentation that came with your application.

Licensing Forcepoint NGFW components

Generate and download a license for each SMC server and NGFW Engine node before you start installing the Forcepoint NGFW.

You install the SMC server license when you start the SMC after installation. You install the NGFW Engine licenses when you start configuring the NGFW Engines.

Types of licenses for SMC servers and NGFW Engines

Each SMC server and NGFW Engine node must have its own license.

- Some NGFW Engines use an NGFW Engine Node license. Other NGFW Engines use role-specific licenses. The correct type of license for each NGFW Engine is generated based on your Management Server proof-of-license (POL) code or the appliance proof-of-serial (POS) code.
- If there is no connection between the Management Server and the License Center, a Forcepoint NGFW appliance can be used without a license for 30 days. After this time, you must generate the licenses manually at the License Center webpage and install them using the Management Client.
- Virtual NGFW Engines do not require a separate license. However, the Master NGFW Engine license limits the number of Virtual Resources that can be created. The limit for the number of Virtual Resources defines how many Virtual NGFW Engines can be created.
- The Management Server's license might be limited to managing only a specific number of NGFW Engines.
- Forcepoint NGFW Engines deployed in the AWS cloud with the Bring Your Own License image must have a license in the SMC. Forcepoint NGFW Engines deployed in the AWS cloud with the Hourly (pay as you go) image do not require a separate license in the SMC.

Licenses can be bound to a component in several different ways. The possible binding methods depend on the licensed component and the software version.

License binding methods

License binding	Description
IP address binding	The license is statically bound to the IP address of the licensed component. **Note** Only licenses for SMC servers can be bound to an IP address. Existing IP-address-bound licenses for other components continue to work and can be upgraded. Any new licenses for other components must be bound to the Management Server's proof-of-license (POL) code.
UIID binding	The license is statically bound to the unique installation identifier (UIID) for the SMC. The UIID is automatically generated when you install the SMC. The UIID is also shown in the properties of the Management Server, Log Server, or Web Portal Server elements. **Note** Only licenses for SMC servers can be bound to the UIID for the SMC.
Management Server proof-of-license (POL) code binding	Licenses are dynamically bound to the Management Server's proof-of-license (POL) code. You must manually bind Management Server POL-bound licenses to the correct element. Licenses are valid only for components that are managed by the Management Server that has the same POL code.

License binding	Description
Appliance proof-of-serial (POS) code binding	The license is bound to the unique POS code of a pre-installed Forcepoint NGFW appliance. The appliance identifies itself when contacting the Management Server. The Management Server allows the use of the appliance if the license POS code matches the reported code. The Management Server automatically binds the correct license to the NGFW Engine element based on the POS code. For the Management Server and pre-installed appliances, the Management Server can use this licensing method automatically with new appliances.

The license types that are available depend on the SMC server or type of NGFW Engine.

License binding	Description
Management Servers	A static IP-address-bound license or a static UIID-bound license.
Log Servers	A static IP-address-bound license, a static UIID-bound license, or a dynamic license bound to the Management Server's POL code
Web Portal Servers	
Pre-installed Forcepoint NGFW appliances	A license bound to the POS code of the appliance (all current models) or a dynamic license bound to the Management Server's POL code (older models)
NGFW Engines installed on your own hardware	Always a dynamic license bound to the Management Server's POL code
NGFW Engines installed on a virtualization platform	Always a dynamic license bound to the Management Server's POL code
Feature-specific licenses	A dynamic license bound to the Management Server's POL code or a license bound to the POS code of the appliance depending on the feature

After the NGFW Engines and the SMC are fully installed, the SMC can automatically download and install future NGFW Engine licenses. For more information about automatic downloading and installation of licenses, see the *Forcepoint Next Generation Firewall Product Guide*.

Obtain license files

Generate the licenses based on your Management Server proof-of-license (POL) code or the appliance proof-of-serial-number (POS) code.

If you are licensing several components of the same type, remember to generate a license for each component.

Evaluation licenses are also available. Evaluation license requests might need manual processing. See the license page for current delivery times and details.

All licenses include the latest version for which they are valid. Automatic upgrade and installation of licenses is enabled by default. If you have disabled automatic license upgrades, you must upgrade the licenses when you upgrade to a new major release of the software.

Steps

1) Go to https://stonesoftlicenses.forcepoint.com.

2) In the **License Identification** field, enter the POL or POS code, as follows.
   - Proof-of-license (POL) code — Identifies the license. For previously licensed components, the POL code is shown in the Licenses tree in the **Administration Configuration** view.

- Proof-of-serial (POS) number — The Forcepoint NGFW appliances additionally have a proof-of-serial number that you can find on a label attached to the appliance hardware.

3) Click **Submit**.

4) Check which components are listed as included in this license, then click **Register**.

5) Read the instructions on the page, then fill in the required fields for all included components.

6) Enter the details that bind each license to a component, as follows:

Component	Details for license binding
Management Servers	■ IP-address-bound license — Enter the IP address that you plan to use on the server. If your license allows several Management Servers in the same SMC for high availability, enter a comma-separated list of the IP addresses of all Management Servers. ■ UIID-bound license — Enter the UIID of the SMC. The UIID is automatically generated when you install the SMC. The UIID is also shown in the properties of the Management Server, Log Server, or Web Portal Server elements.
Other SMC servers	■ IP-address-bound license — Enter the IP address that you plan to use on the server. ■ Management Server POL-bound license — Enter the Management Server's POL code. ■ UIID-bound license — Enter the UIID of the SMC. The UIID is automatically generated when you install the SMC. The UIID is also shown in the properties of the Management Server, Log Server, or Web Portal Server elements.
Master NGFW Engines	Enter the POS code of a Forcepoint NGFW appliance (see the label attached to the appliance).
NGFW Engines	■ For Forcepoint NGFW appliances, enter the POS code of the appliance (see the label attached to the appliance). ■ For Forcepoint NGFW software installed on your own hardware or on a virtualization platform, enter the POL code of the Management Server that you use to manage the NGFW Engine. **Note** POS binding is always recommended when the option is available.

Note

If the binding information is incorrect, the license is unusable. If you accidentally generated a license with the wrong binding information, request a license change through the License Center.

7) Click **Submit Request**.
The license file available for download at the License Center.

Related tasks

Install licenses for SMC servers on page 58
Install licenses for NGFW Engines on page 78

Installation overview

The process of installing Forcepoint NGFW consists of several high-level steps.

1) Install and configure the SMC and a Management Client.

2) Download licenses for the SMC components and the NGFW Engines, and install the licenses in the Management Client.

3) If network address translation (NAT) is applied to communications between system components, define contact addresses for the SMC components in the Management Client.

4) Define the Firewalls, IPS engines, and Layer 2 Firewalls in the Management Client. You can optionally define Master NGFW Engines and Virtual NGFW Engines.

5) Configure interfaces and routing for the NGFW Engines in the Management Client.

6) In the Management Client, generate the initial configuration for Firewalls, IPS engines, Layer 2 Firewalls, and Master NGFW Engines. You do not need an initial configuration for Virtual NGFW Engines.

7) If you are not using a Forcepoint appliance that has pre-installed Forcepoint NGFW software, install the NGFW software on virtualization platforms or third-party hardware.

8) Configure the NGFW software and apply the initial configuration to the NGFW Engines.

9) Create and install a policy on the NGFW Engines.

Part II

Security Management Center deployment

Contents

SMC is the management component of the Forcepoint NGFW system. SMC must be installed and running before you can deploy the Forcepoint NGFW engines.

Chapter 3

Installing the SMC

Contents

The SMC is the management component of the Forcepoint NGFW solution. The SMC manages and controls the other components in the system. You must install the SMC before you can install Forcepoint NGFW Engines.

SMC installation options

You can install SMC server components on your own hardware or use an all-in-one SMC Appliance.

CAUTION

Make sure that the operating system version you plan to install on is supported. The supported operating systems for running the SMC are listed in the Security Management Center Release Notes.

There are several ways to install the SMC server components:

- (Recommended) You can install the SMC server components using the Installation Wizard.

  Tip

  To evaluate the Forcepoint Next Generation Firewall system in a simulated network environment, you can install the SMC in demo mode.

- In Linux, you can install the SMC server components from the command line.

  Note

  You need a graphical environment to use the Management Client. Only the SMC server components can run in a command line-only environment.

- The Management Server and a default Log Server are pre-installed on the SMC Appliance. When you start the appliance, the installation wizard includes the configuration of these components.

During the installation, certificates can be generated for the SMC server components. The certificates are needed for authentication in establishing the secure encrypted communication channel between system components.

After the installation, you can install the Management Client on other computers. You can also run the Management Client in a web browser.

Note

For third-party hardware, we recommend installing a Management Client on the same computer as the Management Server.

Related tasks

Install the SMC in Demo Mode on page 47
Install the SMC in Linux from the command line on page 49

Requirements for running SMC on third-party hardware

There are some minimum requirements and recommendations when you run the SMC on third-party hardware.

For more information, see the Release Notes.

Security considerations for SMC deployment

The information stored in the Security Management Center (SMC) is highly valuable to anyone conducting or planning malicious activities in your network. Someone who gains administrator rights to the Management Server can change the configurations.

An attacker can gain access by exploiting operating system weaknesses or other services running on the same computer to gain administrator rights in the operating system.

Important

Secure the Management Server computer. Anyone who has administrator rights to the operating system can potentially view and change any SMC configurations.

Consider at least the following points to secure the Management Server and Log Server:

- Prevent any unauthorized access to the servers. Restrict access to the minimum required both physically and with operating system user accounts.
- We recommend allowing access only to the required ports.
- Never allow Management Client connections from insecure networks.
- Take all necessary steps to keep the operating system secure and up to date.
- We recommend that you do not run any third-party server software on the same computer with the SMC servers.
- We recommend placing the servers in a separate, secure network segment without third-party servers and limited network access.

You can optionally use 256-bit encryption for the connection between the engines and the Management Server. You must also use an Internal ECDSA Certificate Authority to sign certificates for SMC communication.

When you create and use a new Internal ECDSA Certificate Authority to sign certificates for system communication, the Management Server and the engine re-establish their trust relationship. After the

Management Server and the engine re-establish their trust relationship, 256-bit encryption is enabled for the connection between the engines and the Management Server.

Related reference
Forcepoint NGFW Engine ports on page 238
Security Management Center ports on page 235

Basic system settings for the SMC components

Check these operating system settings on the computers that you use as a platform for the SMC components.

Date and time settings for SMC components

Make sure that the date, time, and time zone settings are correct on any computer that you use as a platform for any SMC component, including the Management Client workstations. The time settings of the NGFW Engines do not need to be adjusted, as they are automatically synchronized with the Management Server's time setting. For this operation, the time is converted to UTC time according to the Management Server's time zone setting. The SMC always uses UTC internally.

Hosts file for SMC servers

Due to a restriction of the Java platform, the Management Server and Log Server host names must be resolvable on the computer running the Management Client. This restriction applies even if the Management Client is running on the same computer as the servers.

To guarantee that the host names can be resolved, add the IP address and host name pairs to the local hosts file on the client computer:

- In Windows: `\%SystemRoot%\system32\drivers\etc\hosts`
- In Linux: `/etc/hosts`

Installing on Linux

The installation creates sgadmin user and group accounts.

If there is a pre-existing sgadmin account, the installation fails. All shell scripts belong to sgadmin and are executed either by root or the sgadmin user. The shell scripts are executed with sgadmin rights. After the installation, the sgadmin account is disabled. The sgadmin account is deleted at uninstallation.

SMC installation overview

The process of installing SMC consists of several high-level steps.

1) Install the SMC components or start the SMC Appliance.

If you are installing components on separate computers, install the Management Server first.

2) Start the SMC.

3) Install licenses for SMC servers.

4) (Optional) Install additional Management Servers.

Install the SMC

You can install the SMC using a graphical user interface installation wizard in Windows and Linux.

For information about installing the all-in-one appliance, see the topic about installing the SMC Appliance.

Related tasks

Obtain installation files on page 27
Install the SMC in Linux from the command line on page 49
Install the SMC Appliance on page 54

Start the installation

Start the Installation Wizard on the computer where you want to install the SMC components.

Steps

1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.

2) Start the Installation Wizard from a .zip file or the Installation DVD.
Decompress the .zip file.
   - On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
   - On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

   If the DVD is not automatically mounted in Linux, use the following command:

   ```
   mount /dev/cdrom /mnt/cdrom
   ```

3) Select the language for the installation, then click **OK**.
The language that you select is also set as the default language of the Management Client.

4) Read the information on the **Introduction** page, then click **Next**.

   Tip

   Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.

5) Select **I accept the terms of the License Agreement**, then click **Next**.

6) (Optional) Select where to install the SMC, then click **Next**.

The default installation directory in Windows is `C:\Program Files\Forcepoint\SMC`. Click **Choose** to browse to a different installation folder.

Note

If you install the SMC in `C:\Program Files\Forcepoint\SMC`, the installation creates an extra `C:\ProgramData\Forcepoint\SMC` folder, which duplicates some of the folders in the installation directory and also contains some of the program data.

7) (Linux only) Read the instructions about the hosts file, make any necessary configuration changes, then click **Next**.

8) Select where to create shortcuts, then click **Next**.

These shortcuts can be used to manually start components and to run some maintenance tasks.

9) Select the installation type, then click **Next**.

- **Typical** — Installs a Management Server, a Log Server, and the Management Client.
- **Management Client Only** — Use to install additional Management Clients on administrators' workstations.
- **Demo Mode** — For more information, see the section about installing in Demo mode.
- **Custom** — Select individual components to install. Use this option to:
  - Install individual SMC components. For example, you can install the Management Server on one computer, and the Log Server on another.
  - Install the Web Portal Server.
  - Install the Cloud Discovery tool.
  - Install only a Management Server if you want to install an additional Management Server for high availability.

10) If you selected a custom installation, select the components to install, then click **Next**.

Important

Make sure that you have a license for any separately licensed components before installing them. The Web Portal Server is not included in standard SMC licenses.

Install a Management Server

Continue the installation in the Installation Wizard to configure the options for the Management Server.

Steps

1) Configure the settings, then click **Next**.

Option	Description
Select Management Server IP Address	Select the server's IP address from the drop-down list. If you use IP address binding, the server's license must be generated with this IP address as the binding.
Log Server IP Address	Enter the IP address of the Log Server to which this server sends its log data.
Advanced Management Server Options	When selected, you can configure additional options on another page. Select this option if you want to: ■ Disable the use of 256-bit encryption for communication between the Management Server and the NGFW Engines. ■ Enable the use of SMC Web Access to run the Management Client in a web browser. ■ (Linux only) Enable integrating NSX-V with Forcepoint NGFW.
Install as an Additional Management Server for High Availability	When selected, you can configure additional options on another page. For more information, see the section about adding a Management Server for high availability.
Enable FIPS 140-2 Configuration Restrictions	When selected, FIPS 140-2 restrictions are enabled. **Note** This option only is for environments that are required to follow the FIPS 140-2 standards. Do not select this option unless you have a specific reason to do so.
Install the Management Server as a Service	When selected, the server starts automatically.

2) If you selected **Advanced Management Server Options** on the previous page, select the features to enable, then click **Next**.

Option	Description
Enable and Configure SMC Web Access	When enabled, administrators can access the SMC in a web browser. You can run the Management Client in a web browser instead of installing the Management Client locally. On Linux platforms, xvfb-run must be installed under `/usr/bin`. You can specify another path in the Management Server properties after the installation has completed.
Enable NSX Service (Linux only)	When enabled, allows integrating NSX-V with Forcepoint NGFW.
256-bit Security Strength	When enabled, 256-bit encryption is used for communication between the Management Server and the NGFW Engines. This option is selected by default.

3) If you enabled SMC Web Access, configure the settings, then click **Next**.

Option	Description
Port Number	Enter the TCP port number that the service listens to. By default, port 8085 is used when SMC Web Access is enabled on the Management Server and port 8083 when enabled on the Web Portal Server. **Note** Make sure that the listening port is not in use on the server.
Host Name (Optional)	Enter the host name that the service uses. Leave the field blank to allow requests to any of the server's host names.
Certificate Distinguished Name	Administrators must use an HTTPS connection to access and use the Management Client. Enter the distinguished name for the certificate used to secure the HTTPS connection.
Certificate Algorithm	Select the algorithm and key length for the certificate used to secure the HTTPS connection.
Certificate Signer	Select the signer for the certificate used to secure the HTTPS connection. You can use the Internal Certificate Authority or the certificate can be self-signed.

4) Enter a user name and password to create a superuser account, then click **Next**.

Important

This is the only account that an administrator can use to log on after the installation has been completed.

Install a Log Server

Continue the installation in the Installation Wizard to configure the options for the Log Server.

Steps

1) Configure the settings, then click **Next**.

Option	Description
Select Log Server IP Address	Select the server's IP address from the drop-down list. If you use IP address binding, the server's license must be generated with this IP address as the binding.
IP Address(es) of the Management Server(s) that will control this Log Server	Enter the IP address of the Management Server that controls this server. If there are multiple Management Servers, enter the IP addresses as a comma-separated list.
Certify the Log Server during the installation	When selected, the server is automatically certified. If the components are installed on different computers and the Management Server is not immediately contactable, deselect this option to avoid connection attempts after installation. Certifying is mandatory for running the server.
Port on which the Log Server will receive data	Enter the port number that the server receives data on.
Enable FIPS 140-2 Configuration Restrictions	When selected, FIPS 140-2 restrictions are enabled. **Note** This option only is for environments that are required to follow the FIPS 140-2 standards. Do not select this option unless you have a specific reason to do so.
Install the Log Server as a Service	When selected, the server starts automatically.

2) (Optional) Click **Choose** to browse to a different storage folder for log data.

Note

Remote locations are not suitable for active storage, as quick and reliable access is required.

3) Click **Next**.

Install a Web Portal Server

Continue the installation in the Installation Wizard to configure the options for the Web Portal Server. The Web Portal Server provides restricted access to log data, reports, and policy snapshots.

Before you begin

Make sure that you have a license for the Web Portal Server before installing it. The Web Portal Server is an optional component and is not included in standard Security Management Center licenses.

Steps

1) Configure the settings, then click **Next**.

Option	Description
Select Web Portal Server IP Address	Select the server's IP address from the drop-down list. If you use IP address binding, the server's license must be generated with this IP address as the binding.
IP Address(es) of the Management Server(s) that will control this Web Portal Server	Enter the IP address of the Management Server that controls this server. If there are multiple Management Servers, enter the IP addresses as a comma-separated list.
Certify the Web Portal Server during the installation	When selected, the server is automatically certified. If the components are installed on different computers and the Management Server is not immediately contactable, deselect this option to avoid connection attempts after installation. Certifying is mandatory for running the server.
Log Server IP Address	Enter the IP address of the Log Server to which this server sends its log data.
Enable FIPS 140-2 Configuration Restrictions	When selected, FIPS 140-2 restrictions are enabled.  **Note** This option only is for environments that are required to follow the FIPS 140-2 standards. Do not select this option unless you have a specific reason to do so.
Install the Web Portal Server as a Service	When selected, the server starts automatically.

Install the Cloud Discovery Tool

Continue the installation in the Installation Wizard to configure the options for the Cloud Discovery Tool. The tool can process log data exported from the SMC to produce a summary report about cloud application usage.

Before you begin

Make sure that you have a license for the Cloud Discovery Tool. The Cloud Discovery Tool is an optional component and is not included in standard SMC licenses. To get the license, you must contact your Forcepoint sales representative.

Note

You cannot install the Cloud Discovery Tool as the only SMC component. You must install at least one other SMC component to install the Cloud Discovery Tool.

To use exported log data with the Cloud Discovery Tool, the data must be in Short CSV format.

Steps

1) Select the working directory for running the Cloud Discovery report from exported log data.
2) Next to the **Upload License** field, click **Choose**, then browse to the location of the license file.
3) Click **Next**.

Finish the installation

Review the configuration options that you set in the Installation Wizard, then finish the installation.

Before you begin

If you are installing any server components as a service on a Windows system, make sure that the Services window is closed before you proceed.

Important

This is the last chance to cancel the installation or make changes. Click **Previous** to adjust your selections.

Steps

1) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.

   Depending on the options, you selected, you might be prompted to generate certificates during the installation.

   When the installation has completed, the unique installation identifier (UIID) for the SMC is shown. If you plan to use UIID-bound licenses for SMC servers, make a note of the UIID for the SMC. You will need the UIID to generate licenses.

2) When the installation has completed, click **Done**.

   Note

   If any Log Server or Web Portal Server certificate was not retrieved during the installation, retrieve a certificate manually before starting the server.

Related tasks

Generate SMC server certificates on page 60

Install the SMC in Demo Mode

The Demo Mode installation creates a simulated network environment for evaluation.

Demo Mode installation is for evaluation only. The SMC in Demo mode cannot be used for traffic inspection and cannot be upgraded.

Steps

1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.

2) Start the Installation Wizard from a .zip file or the Installation DVD.

   Decompress the .zip file.

   - On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
   - On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

   If the DVD is not automatically mounted in Linux, use the following command:

   ```
   mount /dev/cdrom /mnt/cdrom
   ```

3) Select the language for the installation, then click **OK**.

   The language that you select is also set as the default language of the Management Client.

4) Read the information on the **Introduction** page, then click **Next**.

   Tip

   Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.

5) Select **I accept the terms of the License Agreement**, then click **Next**.

6) (Optional) Select where to install the SMC, then click **Next**.

The default installation directory in Windows is `C:\Program Files\Forcepoint\SMC`. Click **Choose** to browse to a different installation folder.

Note

If you install the SMC in `C:\Program Files\Forcepoint\SMC`, the installation creates an extra `C:\ProgramData\Forcepoint\SMC` folder, which duplicates some of the folders in the installation directory and also contains some of the program data.

7) (Linux only) Read the instructions about the hosts file, make any necessary configuration changes, then click **Next**.

8) Select where to create shortcuts, then click **Next**.

These shortcuts can be used to manually start components and to run some maintenance tasks.

9) Select **Demo Mode** as the installation type, then click **Next**.

10) Select the **Standard** demo backup to simulate a standard preconfigured environment, then click **Next**.

You can also use the **Select your own backup file** option to create the simulation based on your environment.

11) Read the description of the Demo Mode installation, then click **Next**.

12) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.

13) When the installation has completed, click **Done**.

Result

The Management Client starts automatically, and the simulated environment is now ready for testing.

Related tasks

Log on to the SMC on page 57

Install the SMC in Linux from the command line

In Linux, you can install the Security Management Center on the command line.

Before you begin

Check the installation package integrity using the file checksums.

Important

You need a graphical environment to use the Management Client. It cannot be run on the command line. Only the SMC server components can be run in a command line-only environment.

Related tasks

Check file integrity on page 28

Start the installation on the command line

Start the command line installer to install SMC components from the command line.

Steps

1) Log on to the operating system as the root user.

2) Start the Installation Wizard from a .zip file or the Installation DVD.
Decompress the .zip file.
If the DVD is not automatically mounted, use the following command:

```
mount /dev/cdrom /mnt/cdrom
```

The path to the installer is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`. Run the script with the `-nodisplay` parameter.
When using the installer, enter `back` to return to the previous step or `quit` to cancel the installation.

3) Select the language for the installation.
To use the default option, press **Enter**. You can also select another option, then press **Enter**.

4) Read the information in the introduction, then press **Enter**.

5) Press **Enter** to scroll through the license agreement, then enter `Y` to accept the license agreement.

6) Specify the installation directory.
To use the default option, press **Enter**. You can also enter a different directory, then press **Enter**.

7) Read the instructions about the hosts file, make any necessary configuration changes, then press **Enter**.

8) Create links to the most commonly used command-line tools.
To use the default option, press **Enter**. You can also select another option, then press **Enter**.

9) Select the type of installation.
   - **Typical** — Installs a Management Server, a Log Server, and the Management Client.
   - **Management Client Only** — Use to install additional Management Clients on administrators' workstations.
   - **Demo Mode** — For more information, see the section about installing in Demo mode.
   - **Custom** — Select individual components to install. Use this option to:
     - Install individual SMC components. For example, you can install the Management Server on one computer, and the Log Server on another.
     - Install the Web Portal Server.
     - Install the Cloud Discovery tool.
     - Install only a Management Server if you want to install an additional Management Server for high availability.

10) If you selected a custom installation, enter a comma-separated list of numbers that represent the components you want to install, then press **Enter**.
   - Enter the number of a *selected* component to *deselect* the component.
   - Enter the number of a component that is *not* selected to *select* the component.
   - By default, the Management Server, Log Server, and Management Client are selected.

   For example, to install only the Web Portal Server, enter `1,2,3,4`, then press **Enter**.

11) Review the component selection, then press **Enter**.

Install a Management Server on the command line

Configure the Management Server settings in a command line installation.

Steps

1) Specify the IP address for the server.
To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**.
If IP address binding is used, the server's license must be generated with this IP address as the binding.

2) Specify the IP address for the Log Server to which the server sends its log data.
To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**.

3) To install as an additional Management Server for high availability, enter `Y`.
To install as a standalone Management Server or as the primary Management Server in a high-availability environment, enter `N`.

4) To enable and configure SMC Web Access, enter `Y`. Otherwise, enter `N`.

When enabled, administrators can access the SMC in a web browser. You can run the Management Client in a web browser instead of installing the Management Client locally.

On Linux platforms, xvfb-run must be installed under `/usr/bin`. You can specify another path in the Management Server properties after the installation has completed.

5) If you enabled SMC Web Access, configure the settings.

Administrators must use an HTTPS connection to access and use the Management Client.

a) Enter the TCP port number that the service listens to.

By default, port 8085 is used when SMC Web Access is enabled on the Management Server and port 8083 when enabled on the Web Portal Server.

Note

Make sure that the listening port is not in use on the server.

b) Enter the host name that the service uses. Leave the field blank to allow requests to any of the server's host names.

c) Enter the distinguished name for the certificate used to secure the HTTPS connection.

d) Select the algorithm and key length for the certificate used to secure the HTTPS connection.

To use the default option, press **Enter**. You can also select another option, then press **Enter**.

e) Select the signer for the certificate used to secure the HTTPS connection.

You can use the Internal Certificate Authority or the certificate can be self-signed. To use the default option, press **Enter**. You can also select another option, then press **Enter**.

6) To enable 256-bit security strength for communication between the Management Server and NGFW Engines, enter `Y`. Otherwise, enter `N`.

7) (256-Bit Security Strength only) If you are shown a compatibility warning, press **Enter** to continue, or type `back` to restart the Management Server configuration and disable 256-bit security strength.

8) To enable integrating NSX-V with Forcepoint NGFW, enter `Y`. Otherwise, enter `N`.

9) To enable FIPS 140-2 restrictions, enter `Y`. Otherwise, enter `N`.

Note

This option only is for environments that are required to follow the FIPS 140-2 standards. Do not select this option unless you have a specific reason to do so.

10) To install the server as a service, enter `Y`. Otherwise, enter `N`.

When installed as a service, the server starts automatically.

11) To create a superuser account, enter a user name, then enter and confirm the password.

Related information
Default communication ports on page 235

Install a Log Server on the command line

Configure the Log Server settings in a command line installation.

Steps

1) Specify the IP address for the server.
   To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**.
   If IP address binding is used, the server's license must be generated with this IP address as the binding.

2) Specify the IP address of the Management Server that controls this server.
   To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**. If there are multiple Management Servers, enter the IP addresses as a comma-separated list.

3) Specify the port on which the Log Server receives data.
   To use the default option, press **Enter**. You can also enter a different port, then press **Enter**.

4) To install the server as a service, enter `Y`. Otherwise, enter `N`.
   When installed as a service, the server starts automatically.

5) Specify the directory for storing log files.
   To use the default option, press **Enter**. You can also enter a different directory, then press **Enter**.

Install a Web Portal Server on the command line

Configure the Web Portal Server settings in a command line installation.

Steps

1) Specify the IP address for the server.
   To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**.
   If IP address binding is used, the server's license must be generated with this IP address as the binding.

2) Specify the IP address of the Management Server that controls this server.
   To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**. If there are multiple Management Servers, enter the IP addresses as a comma-separated list.

3) Specify the IP address for the Log Server to which the server sends its log data.
   To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**.

4) To install the server as a service, enter `Y`. Otherwise, enter `N`.
When installed as a service, the server starts automatically.

Install the Cloud Discovery Tool on the command line

Configure the Cloud Discovery Tool settings in a command line installation.

Before you begin

Make sure that you have a license for the Cloud Discovery Tool. The Cloud Discovery Tool is an optional component and is not included in standard SMC licenses. To get the license, you must contact your Forcepoint sales representative.

Note

You cannot install the Cloud Discovery Tool as the only SMC component. You must install at least one other SMC component to install the Cloud Discovery Tool.

To use exported log data with the Cloud Discovery Tool, the data must be in Short CSV format.

Steps

1) Enter the path to the working directory for running the Cloud Discovery report from exported log data, then press **Enter**.
To use the default option, press **Enter**. You can also enter a different directory, then press **Enter**.

2) Enter the path to the license file, then press **Enter**.
To use the default option, press **Enter**. You can also enter a different directory, then press **Enter**.

Finish the installation on the command line

Review the configuration options that you set in the command line installer, then finish the installation.

Important

This is the last chance to cancel the installation or make changes. Enter `back` to adjust your selections, or enter `quit` to cancel the installation.

Steps

1) Check that the information in the **Pre-Installation Summary** is correct, then press **Enter**.

Result

The components that you selected are installed.
When the installation has completed, the unique installation identifier (UIID) for the SMC is shown. If you plan to use UIID-bound licenses for SMC servers, make a note of the UIID for the SMC. You will need the UIID to generate licenses.

Install the SMC Appliance

The SMC Appliance ships with the Management Server and a Log Server pre-installed on it. Starting the SMC Appliance initiates an installation wizard.

Before you begin

Prepare the appliance for installation:

- Determine the appliance networking information:
  - IPv4 network addresses
  - IPv4 network masks
  - (Optional) Default gateway address
  - (Optional) DNS server addresses
- Mount the appliance in a rack.
- Connect the network and console cables.
- Access the appliance through a KVM or the integrated Dell Remote Access Controller (iDRAC) port.

See the *Forcepoint NGFW Security Management Center Appliance Hardware Guide* for complete details.

Steps

1) Turn on the SMC Appliance.

2) Select the keyboard layout for accessing the SMC Appliance on the command line.

3) Accept the EULA.

4) Enter the account name and password.

   The password must be at least ten characters long and contain at least one number. The account name and password become an administrator account with unrestricted permissions (superuser) on the Management Server.

   a) Enter the account name.

      This field is case sensitive and limited to eight characters.

   b) Enter the password.

      The password is case sensitive and must have a minimum of ten characters.

c) Enter the password again.

5) (Optional) Configure a bootloader password.

If you configure a bootloader password, you must enter the bootloader password to edit the options that appear in the bootloader menu of the SMC Appliance.

a) Enter `Y` to configure a bootloader password.

b) Enter the password.

c) Enter the password again.

6) Make your security selections.

a) Specify if the appliance runs in FIPS 140-2 mode.

No is the default.

Note

This option is for environments that are required to follow the FIPS 140-2 standards.

b) Specify if the appliance uses 256-bit security strength.

Yes is the default.

Note

The security strength is for the connection to the NGFW Engines. The engines must also use 256-bit security strength.

7) Select whether to configure a secondary management interface.

8) Complete the network interface and network setup fields for the main network interface.

a) Select the main network interface for management.

b) Complete the network setup fields for the interface.

9) (Secondary management interface only) Complete the network interface and network setup fields for the second network interface for management.

a) Select the main network interface for management.

b) Complete the network setup fields for the interface.

10) Enter a host name for the Management Server.

11) Select the time zone.

12) Set the time.

13) (Optional) Configure NTP settings.

Note

NTP settings that you configure in the installation wizard are not visible in the Management Client. Configuring NTP in the Management Client overrides the NTP settings that you configure here.

Result

When the installation is complete, the SMC Appliance restarts.

Related tasks

Contact the Management Server on the command line on page 194

Start the SMC after installation

Proceed through the following sections to start the SMC for the first time.

Start the Management Server

If the Management Server does not start automatically, you must start it.

If the Management Server has been installed as a service, it starts automatically both after the installation and during the operating system boot process. In Windows, the Forcepoint NGFW Management Server service is controlled in the **Services** window, under the **Administrative Tools** category of the Windows Control Panel.

Steps

1) Start the Management Server manually.
   - In Windows, use the shortcut icon or run the script `<installation directory>/bin/sgStartMgtSrv.bat`.
   - In Linux, run the script `<installation directory>/bin/sgStartMgtSrv.sh`.

Next steps

When the Management Server has successfully started, start the Management Client.

Start the Management Client

After you have started the Management Server, start the Management Client.

Steps

1) If you installed the Management Client locally on the workstation, do the following:
   - (Windows) Use the shortcut icon or run the script `<installation directory>/bin/sgClient.bat`.

- (Linux) Run the script `<installation directory>/bin/sgClient.sh`. A graphical environment is needed.

2) If you enabled SMC Web Access to run the Management Client in a web browser, do the following:

   a) In a web browser, browse to the URL of the server that you configured the SMC Web Access feature on.

   The URL can be the IP address of the server or the host name that you defined in the properties of the server. Make sure that you include the port number at the end of the URL.

   Example where SMC Web Access is enabled on the default port 8085 on the Management Server: `https://127.0.0.1:8085`

   b) Enter your user name and password, then click **Log On**.

Log on to the SMC

The Management Client connects to the Management Server and to Log Servers.

Steps

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

1) Select the Management Server in one of the following ways.
   - Select an existing Management Server IP address or DNS name.
   - Click **Add Management Server**, then enter the IP address or DNS name of the Management Server.

   In Demo mode, select 127.0.0.1.

2) Enter the user name and password for the Administrator you defined during the Management Server or SMC Appliance installation.

   In Demo Mode, both the user name and password are "demo".

   Note

   In FIPS mode, previously used user names are not shown in the logon dialog box.

3) Click **Log On**.

Result

After you log on to the Management Client, the Management Client shows the date and time when you last logged on to the Management Client, and the IP address from which you last logged on. If your administrator permissions have been changed since the last time you logged on, you are notified that your permissions have been changed.

Accept the Management Server certificate

As a precaution, to make sure that you are communicating with your Management Server, check the Certificate Authority fingerprint.

The certificate dialog box that contains the fingerprint is shown when the Management Client contacts a Management Server for the first time. You can also manually view the fingerprint.

Steps

1) View the Management Server fingerprint.
   - In Windows, use the shortcut icon (default: **Start** > **All Programs** > **Forcepoint** > **Show Fingerprint**) or run the script `<installation directory>/bin/sgShowFingerPrint.bat`.
   - In Linux, run the script `<installation directory>/bin/sgShowFingerPrint.sh`.
   - On the SMC Appliance, log on to the command line with your administrator credentials, then run the following command

     ```
     sudo /usr/local/forcepoint/smc/bin/sgShowFingerPrint.sh -nodisplay
     ```

2) If the fingerprint matches, click **Accept**.

Result

The Management Client starts.

Install licenses for SMC servers

Install the SMC server licenses that you downloaded while preparing for installation.

The SMC servers require licenses to become operational. If you do not have a valid Management Server license, a message appears when you log on. If the message appears after licensing, make sure that the license binding details are correct.

- If you use IP address binding, make sure that the IP addresses are correct and active on the server when the Management Server service starts.
- If you use licenses bound to the unique installation identifier (UIID) for the SMC, make sure that the UIID that you used to generate the license matches the UIID shown in the properties of the SMC server element.

Steps

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

1) In the Management Client, install licenses through the License Information message.
   a) Click **Continue**.

   b) Select the license files in the dialog box.

      If the message is not shown, install the licenses as explained in the next step. Otherwise, check that the licenses were installed correctly.

2) If you are not prompted to install a Management Server license, install the license files for the other SMC servers.
   a) Select ☰ **Menu** > **System Tools** > **Install Licenses**.
   b) Select the license files and click **Install**.
3) To check that the licenses were installed correctly, select ⚙ **Configuration**, then browse to **Administration** > **Licenses** > **All Licenses**.

Related tasks
Obtain license files on page 31

Bind Management Server POL-bound licenses to servers

You must bind Management Server POL-bound licenses for Log Servers and Web Portal Servers to specific Server elements.

Steps

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

1) Select ⚙ **Configuration**, then browse to **Administration**.
2) Browse to **Licenses** > **Servers**.
3) Right-click a Management Server POL-bound license, then select **Bind**.
4) In the **Select License Binding** dialog box, select the correct server from the list, then click **Select**.

Tip

If you bound the license to an incorrect element, right-click the license, select **Unbind**.

Note

The license is permanently bound to the Log Server or Web Portal Server element when the server is started for the first time. A permanently bound license cannot be rebound to a different Log Server or Web Portal Server element without relicensing or deleting the element that the license is bound to. Until you do that, the unbound license is shown as **Retained**.

Result

The license is now bound to the selected Log Server or Web Portal Server element.

Start SMC servers

If the Log Server or Web Portal Server does not start automatically, you must manually start them.

If a server has been installed as a service, the server starts automatically during the operating system boot process. If the operating system is restarted and the servers do not yet have a license, you might need to start them manually.

Steps

1) Start the Log Server or the optional Web Portal Server.
   - If you installed the server as a service in Windows, start or stop the server through the **Services** window.
   - You can also run a script from the `<installation directory>/bin/` directory in a console window.

Server type	Windows script	Linux script
Log Server	`sgStartLogSrv.bat`	`sgStartLogSrv.sh`
Web Portal Server	`sgStartWebPortalServer.bat`	`sgStartWebPortalServer.sh`

   Read the console messages for information about the progress. Closing the console stops the service.

2) If the Log Server or Web Portal Server does not start, troubleshoot and resolve issues that cause starting to fail.
   - Try starting the server by running scripts in a console window to see if an error is displayed on the console.
   - Check that licenses are correctly bound to components.
   - Make sure that the server has a valid certificate for secure system communications. If there are certificate-related problems or problems you are not able to identify, try regenerating the certificate.

Generate SMC server certificates

If necessary, you can manually certify an SMC server or generate an SMC server certificate.

To manually certify a server, run one of the following scripts from the `<installation directory>/bin/` directory in a console window.

Server type	Windows script	Linux script
Log Server	sgCertifyLogSrv.bat	sgCertifyLogSrv.sh
Web Portal Server	sgCertifyWebPortalServer.bat	sgCertifyWebPortalServer.sh

To generate a server certificate, follow these steps:

Steps

1) Enter the user name and password for the account you created during the Management Server installation.
   You can also use other accounts that have unrestricted permissions.

2) Click **Accept** to accept the certificate fingerprint of the Management Server's Certificate Authority.
   As a precaution, you can make sure that the communication really is with your Management Server.

3) In the **Server Selection** dialog box, identify the component that you want to certify.
   - If the server element that represents the component is listed, select it.
   - If **recommended** follows the name of a server element, the component ID of the server element matches the ID of the component that you are certifying. We recommend that you select that server element.

     CAUTION

     Selecting a server element that is not the recommended server element might cause serious problems. For example, the server's log data or the monitoring status of the server might be displayed incorrectly.
   - If the correct server element is not listed, select **Create a New Log Server** or **Create a New Web Portal Server**, then enter a name for the server.

4) Click **OK**.

Post-installation SMC configuration

After installation, you can configure settings for system communication and enable more features for the SMC.

- If NAT is applied to communications between any SMC components, configure NAT addresses for SMC components.
- You can install and configure additional Management Servers for high availability.

When you are finished configuring the SMC, you are ready to use the Management Client to configure Firewall, IPS, and Layer 2 Firewall elements. The elements must be configured before installing the physical appliances.

Related concepts

Configuring NAT addresses for SMC components on page 63

Alternative methods for accessing the Management Client

Related tasks

Install additional Management Servers for high availability on page 66

Chapter 4

Configuring the SMC

Contents

After initial installation is complete, configure the SMC to allow adding the other components for your system.

Configuring NAT addresses for SMC components

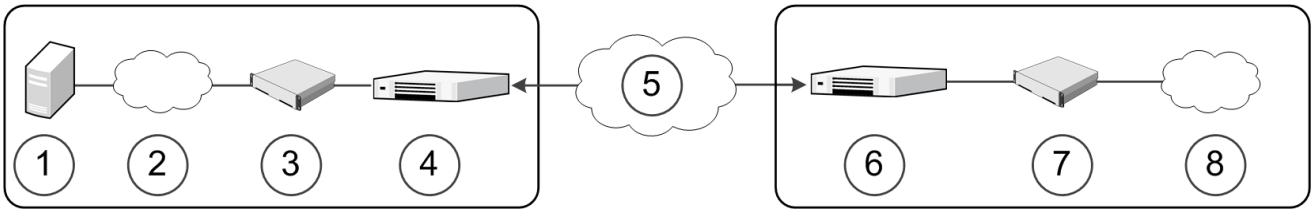
You must configure Locations and contact addresses when network address translation (NAT) is applied to the communications between any of the SMC components.

If there is NAT between communicating SMC components, the translated IP address might have to be defined for system communications.

You use Location elements to configure SMC components for NAT. There is a Default Location to which all elements belong if you do not assign them to a specific Location. If NAT is applied between two SMC components, you must separate them into different Locations and then add a contact address for the component to be contacted.

You can define a Default contact address for contacting an SMC component (defined in the **Properties** dialog box of the corresponding element). The component's Default contact address is used in communications when SMC components that belong to another Location contact the component and the component has no contact address defined for its Location.

Example scenario—using locations



Component	Description
Headquarters Location	
1	Management/Log server
2	Internet

Component	Description
3	IPS
4	Firewall
Between locations	
5	Internet
Branch Office Location	
6	Firewall
7	IPS
8	Internet

In the example scenario above, the same Management Server and Log Server manage SMC components both at a company's headquarters and at the branch office.

NAT could typically be applied at the following points:

- The firewall at the headquarters or an external router can provide the SMC servers external IP addresses on the Internet. The external addresses must be defined as contact addresses so that the SMC components at the branch offices can contact the servers across the Internet.
- The branch office firewall or an external router can provide external addresses for the SMC components at the branch office. In this case, the external IP addresses must also be defined as contact addresses so that the Management Server can contact the components.

When contact addresses are needed, it might be enough to define a single new Location element, for example, for the branch office, and to group the SMC components at the branch office into the "Branch Office" Location. The same Location element could also be used to group SMC components at any other branch office when they connect to the SMC servers at the headquarters.

To be able to view logs, the administrators at the branch office must select the "Branch Office" Location in the Management Client.

Configuration overview

1) Define Location elements.

2) Define contact addresses for the Management Servers and Log Servers.

3) Select the Location for your Management Client.

4) Select the Locations for NGFW Engines when you create the engine elements.

Related information

Default communication ports on page 235

Add Location elements

Group the SMC components into **Location** elements based on which components are on the same side of a NAT device.

The elements that belong to the same **Location** element always use the primary IP address when contacting each other.

Steps

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

1) Select **Configuration**, then browse to **Administration**.
2) Expand the **Other Elements** branch.
3) Right-click **Locations** and select **New Location**.
4) In the **Name** field, enter a name.
5) Select elements from the **Resources** pane and click **Add**.
6) Click **OK**.

Next steps

Continue the configuration in one of the following ways:

- If your **Management Server** or **Log Server** needs a contact address, add SMC server contact addresses.
- Configure the **Firewall**, **IPS**, and **Layer 2 Firewall** elements in the Management Client. You must configure the elements before configuring the Forcepoint NGFW software.

Add SMC Server contact addresses

The Management Server and Log Server can have more than one contact address for each Location.

- If you have additional Management Servers or Log Servers, define two or more contact addresses for each Location. Multiple contact addresses are required so that remote components can connect to a Management Server or a Log Server even if one of the Management Servers or Log Servers fails.
- If you have configured Multi-Link, define two or more contact addresses per Location so that remote components can connect to the servers even if a NetLink goes down.

Steps

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

1) Right-click a server and select **Properties**.
2) From the **Location** drop-down menu, select the location to which the server belongs.

3) If necessary, edit the contact addresses.
   - A Default contact address is automatically entered based on the element properties.
   - If the server has multiple Default contact addresses, separate the addresses with commas.
   - If necessary, click **Exceptions** to define other contact addresses for specific Locations

   Note

   Elements that belong to the same Location element always use the primary IP address when contacting each other instead of any contact addresses. Elements that do not belong to a specific Location are considered to belong to the Default Location.

4) Click **OK**.

Set the Management Client location

When there is a NAT device between the Management Client and a Log Server, select the correct Location for your Management Client. Make the selection in the status bar at the bottom of the Management Client window to be able to view logs.

Note

You must select the Management Client Location separately in each administrative Domain if there are multiple Domains in your environment.

Steps

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

1) In the Management Client, click the **Default Location** name in the status bar at the bottom of the window.

2) Select the Location that includes the IP address or network of the computer where you use the Management Client.

Install additional Management Servers for high availability

You can optionally install one or more additional Management Servers for high availability.

Note

The SMC Appliance does not support high availability for the Management Server or the Log Server.

Additional Management Servers control the system if the active Management Server is damaged, loses power, or becomes otherwise unusable. Configuration data is automatically replicated between the Management Servers. Only one Management Server at a time can be used as an active Management Server to configure and manage the system.

To use additional Management Servers, you must have a special Management Server license that lists the IP addresses of all Management Servers within the same SMC.

Note

You must install the license in the Management Client before installing the additional Management Servers. If you do not yet have the license, generate the license at the Forcepoint website after receiving the Proof-of-License, then install the license.

Steps

1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.

2) Start the Installation Wizard from a .zip file or the Installation DVD.
Decompress the .zip file.
   - On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
   - On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

   If the DVD is not automatically mounted in Linux, use the following command:

   ```
   mount /dev/cdrom /mnt/cdrom
   ```

3) Select the language for the installation, then click **OK**.
The language that you select is also set as the default language of the Management Client.

4) Read the information on the **Introduction** page, then click **Next**.

   Tip

   Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.

5) Select **I accept the terms of the License Agreement**, then click **Next**.

6) (Optional) Select where to install the SMC, then click **Next**.
The default installation directory in Windows is `C:\Program Files\Forcepoint\SMC`. Click **Choose** to browse to a different installation folder.

   Note

   If you install the SMC in `C:\Program Files\Forcepoint\SMC`, the installation creates an extra `C:\ProgramData\Forcepoint\SMC` folder, which duplicates some of the folders in the installation directory and also contains some of the program data.

7) Select where to create shortcuts, then click **Next**.
These shortcuts can be used to manually start components and to run some maintenance tasks.

8) Select **Custom** as the installation type, then click **Next**.

9) Select **Management Server**, then click **Next**.

10) Configure the settings, then click **Next**.

Option	Description
Select Management Server IP Address	Select the server's IP address from the drop-down list. If you use IP address binding, the server's license must be generated with this IP address as the binding.
Log Server IP Address	Enter the IP address of the Log Server to which this server sends its log data.
Advanced Management Server Options	Do not select this option. The options are inherited from the active Management Server.
Install as an Additional Management Server for High Availability	You must select this option.
Enable FIPS 140-2 Configuration Restrictions	When selected, FIPS 140-2 restrictions are enabled. **Note** This option only is for environments that are required to follow the FIPS 140-2 standards. Do not select this option unless you have a specific reason to do so.
Install the Management Server as a Service	When selected, the server starts automatically.

11) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.

12) When prompted during the installation, log on using an unrestricted administrator account.
The Management Server Selection dialog opens.

13) When the Management Server Selection dialog opens, select the correct Management Server from the list, then click **OK**.
You can also select **Create a new Management Server**, then enter a name for the Management Server.
The databases are synchronized.

Note

If the synchronization fails, run the `sgOnlineReplication` script on the additional Management Server when connectivity is restored.

Next steps

- If NAT is applied to communications between any SMC components, configure NAT addresses for SMC components.
- If there is a Firewall or Layer 2 Firewall between the first Management Server you installed and the additional Management Servers, add rules that allow the communications between the servers when you define your Firewall or Layer 2 Firewall Policy.

Related tasks
Install licenses for SMC servers on page 58
Install the SMC on page 40

Using the Management Client in a web browser

To avoid installing the full Java-based Management Client on each workstation that an administrator uses, you can run the Management Client in a web browser.

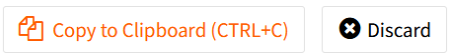
You can enable the SMC Web Access feature on the Management Server or Web Portal Server. Administrators log on to the Management Client on a web page, and the Management Client runs as an HTML5 application in the web browser. The web browser is the only requirement on the workstation.

You can also connect to and manage multiple versions of the SMC. This removes the requirement to have the SMC and the locally-installed Management Client be the same version.

Access is configured in the properties of the Management Server or Web Portal Server. You can also enable the feature during the installation of the Management Server.

Limitations and recommendations

- By default, the SMC allows a maximum of five sessions using SMC Web Access at the same time. To change the maximum number of concurrent sessions, see Knowledge Base article 17248.
- Web browser support is limited to Google Chrome and Mozilla Firefox.
- It is not possible to log on using certificate-based authentication.
- Interacting with the local file system is limited. Each user has a folder located at `%installation%\data\%servertype%\webswing\users\admin%id%` where `%servertype%` is `datamgtserver` for the Management Server and `datawebserver` for the Web Portal Server and `%id%` is the ID of the administrator in the database. Users can import or export elements to this folder, for example.
- When you copy text, using Ctrl+C, you must manually allow the copy operation in the bottom-right corner of the screen.



- SMC Web Access can consume resources. Especially if many administrators will be using the feature, we recommend that you enable the feature on the Web Portal Server.
- If the Management Server or Web Portal Server is installed on a Linux platform, xvfb-run must be installed.
- If the Management Server and Web Portal Server are installed on the same computer, we recommend that you do not enable SMC Web Access on both servers.

Enable SMC Web Access

You can enable and configure the feature in the properties of the Management Server or Web Portal Server.

Note

To use SMC Web Access for a Management Server or Web Portal Server installed on a Linux platform, xvfb-run must be installed in /usr/bin.

Steps

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

1) Select **Configuration**, then browse to **Network Elements**.
2) Browse to **Servers**.
3) Right-click the Management Server or Web Portal Server, then select **Properties**.
4) On the **SMC Web Access** tab, select **Enable**.
5) Configure the settings, then click **OK**.

Management Server and Web Portal Server Properties

Option	Definition
Host Name (Optional)	Enter the host name that the service uses. Leave the field blank to allow requests to any of the server's host names.
Port Number	Enter the TCP port number that the service listens to. By default, port 8085 is used when SMC Web Access is enabled on the Management Server and port 8083 when enabled on the Web Portal Server. **Note** Make sure that the listening port is not in use on the server.
Listen Only on Address (Optional)	If the server has several addresses and you want to restrict access to one address, specify the IP address to use.
Session Timeout	Enter the timeout in seconds after which the session expires. While the session is still active, the administrator does not need to log on again if they close the web browser.
Server Credentials	You must select the TLS Credentials element that is used for HTTPS connections. Click **Select** to select an element.
Use SSL for session ID (Optional)	Track sessions in your web application. Do not select this option if your network requires you to use cookies or URIs for session tracking.

Start the Management Client in a web browser

Administrators can log on to the Management Client and perform their duties using a web browser.

Steps

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

1) In a web browser, browse to the URL of the server that you configured the SMC Web Access feature on.
   The URL can be the IP address of the server or the host name that you defined in the properties of the server. Make sure that you include the port number at the end of the URL.
   Example where SMC Web Access is enabled on the default port 8085 on the Management Server:
   `https://127.0.0.1:8085`

2) Enter your user name and password, then click **Log On**.

3) Use the Management Client as you normally would.

Management Client downloads from the Management Server

When the Management Server provides the Management Client for download, administrators can download and install the Management Client from the SMC Downloads page.

Enable and configure Management Client downloads on the Management Server

To allow administrators to download and install the Management Client from the SMC Downloads page, enable Management Client downloads on the Management Server.

Steps

1) Select **Configuration**, then browse to **Network Elements**.

2) Browse to **Servers**.

3) Right-click the Management Server, then select **Properties**.

4) If it is not already selected, select **Enable** on the **SMC Downloads** tab.

5) Select **Enable Management Client Download**.

6) Configure the settings, then click **OK**.

Management Server Properties	
Option	**Definition**
Host Name (Optional)	Enter the host name that the service uses. Leave the field blank to allow requests to any of the server's host names.
Port Number	Enter the TCP port number that the service listens to. By default, port 8080 is used for new SMC installations, and port 8084 is used when you upgrade the SMC. **Note** Make sure that the listening port is not in use on the server.
Listen Only on Address (Optional)	If the server has several addresses and you want to restrict access to one address, specify the IP address to use.
Server Credentials	You must select the TLS Credentials element that is used for HTTPS connections. Click **Select** to select an element.
Generate Server Logs (Optional)	Select if you want to log all file load events for further analysis with external web statistics software.

Download the Management Client from the Management Server

Download and install the Management Client from the SMC Downloads page.

Steps

1) In a web browser, browse to the URL of the Management Server.
   The URL can be the IP address of the Management Server or the host name that you defined in the properties of the Management Server. Make sure that you include the port number at the end of the URL.

2) To download the Management Client installation package, click **Download Management Client for <operating system>**.

   Tip
   The operating system is automatically detected. To download the Management Client installation package for another operating system, click **Click here for other platforms**.

3) Install the Management Client with administrator privileges.

4) Log on and use the Management Client as you normally would.

Part III

Forcepoint NGFW deployment

Contents

Forcepoint NGFW deployment consists of adding and configuring engine elements in the SMC, and configuring the Forcepoint NGFW software on the engine.

Chapter 5

Configuring Forcepoint NGFW for the Firewall/VPN role

Contents

Configuring engine elements in the SMC prepares the SMC to manage NGFW Engines in the Firewall/VPN role.

Types of interfaces for NGFW Engines in the Firewall/VPN role

You can configure several types of interfaces for NGFW Engines in the Firewall/VPN role.

Types of interfaces for NGFW Engines in the Firewall/VPN role

Interface type	Purpose of interface	Limitations
Layer 3 physical	System communications and traffic inspection.	You cannot add both VLAN Interfaces and IP addresses to a Physical Interface. If an IP address is already configured for a Physical Interface, adding a VLAN Interface removes the IP address. If you plan to use VLAN Interfaces, configure the VLAN Interfaces first and then add IP addresses to the VLAN Interfaces.
Layer 2 physical	Traffic inspection. Layer 2 interfaces on NGFW Engines in the Firewall/VPN role allow the engine to provide the same kind of traffic inspection that is available for NGFW Engines in the IPS and Layer 2 Firewall roles.	You cannot add layer 2 physical interfaces of the Inline Layer 2 Firewall type to Firewall Clusters in Load Balancing mode. Only Standby mode is supported. You cannot add IP addresses to layer 2 physical interfaces on NGFW Engines in the Firewall/VPN role. VLAN retagging is not supported on layer 2 physical interfaces of the inline IPS type.

Interface type	Purpose of interface	Limitations
VLAN	Divides a single physical interface into several virtual interfaces.	■ You cannot add VLAN interfaces on top of other VLAN Interfaces (nested VLANs). ■ You cannot create valid VLAN Interfaces in a Virtual NGFW Engine if the Master NGFW Engine interface that hosts the Virtual NGFW Engine is a VLAN Interface.
ADSL	Represents the ADSL port of a purpose-built Forcepoint NGFW appliance.	An ADSL Interface is only supported on Single Firewall engines that run on specific legacy Forcepoint NGFW appliances that have an ADSL network interface card.
Modem (Single Firewalls only)	Represents a mobile broadband modem connected to a USB port on a purpose-built Forcepoint NGFW appliance.	■ A Modem Interface is only supported on Single Firewall engines that run on specific Forcepoint NGFW appliances. ■ Modem Interfaces do not support VLAN tagging.
Tunnel	A logical interface that is used as an endpoint for tunnels in route-based VPNs.	■ Tunnel Interfaces can only have static IP addresses. ■ Tunnel Interfaces do not support VLAN tagging.
VPN Broker	A specialized interface for use with the VPN Broker. For more information about VPN Broker, see the *Forcepoint NGFW Manager and VPN Broker Product Guide*.	This type of interface is only supported for use with the VPN Broker.
Wireless (Single Firewalls only)	Represents a wireless network interface card of a purpose-built Forcepoint NGFW appliance.	A Wireless Interface is only supported on Single Firewall engines that run on specific Forcepoint NGFW appliances that have a wireless network interface card.
Switch (Single Firewalls only)	Represents the switch functionality on a purpose-built Forcepoint NGFW appliance.	■ The switch functionality is only supported on Single Firewall engines that run on specific Forcepoint NGFW appliances that have an integrated switch. ■ The ports in the integrated switch do not support VLAN tagging or PPPoE. ■ You cannot use ports on the integrated switch as the control interface.

Interface numbering

The interfaces have their own numbering in the SMC called the interface ID. The interface IDs are mapped to the corresponding network interfaces on the NGFW Engine when you configure the Forcepoint NGFW software.

Interface numbering for NGFW Engines

Interface type	Interface numbering in the SMC
Layer 3 physical (Firewall/VPN role)	Each physical interface has a unique interface ID number.
Layer 2 physical (Firewall/VPN role)	
Physical (IPS and Layer 2 Firewall roles)	
VLAN	Each VLAN interface has a VLAN number. The defined VLAN interfaces are displayed, for example, as “5.202” for network interface 5 with VLAN 202.
ADSL	Each ADSL interface has a unique interface ID number. ADSL interfaces are only supported on legacy Forcepoint NGFW appliances.
Wireless	The wireless interface has a unique interface ID number. An SSID (service set identifier) interface represents an 802.11 wireless LAN. You can add several SSID interfaces to the wireless interface.
Modem	Modem Interfaces are identified with modem numbers. The modem number is mapped to the modem’s IMEI (international mobile equipment identity) number. Each modem is assigned a unique ID when you connect the modem to the engine. You can change the mapping between the modem’s IMEI number and the modem ID through the engine command line, if necessary.
Tunnel	Tunnel interfaces are numbered with tunnel interface ID numbers. The mapping of Tunnel Interfaces to physical network interfaces on the engine is done automatically by the engine operating system based on the routing configuration.
Integrated switch	Integrated switches are identified with switch IDs. Integrated switches have predefined switch IDs. For example, the switch ID is 0 on Forcepoint NGFW 110 appliances. You can add port group interfaces to switches. Port group interfaces are identified by port group IDs. The defined switches and port group interfaces are displayed, for example, as *0.1* for switch ID 0 with port group 1.

Install licenses for NGFW Engines

Install the NGFW Engine licenses that you downloaded while preparing for installation.

Before you begin

The license files must be available to the computer that you use to run the Management Client.

You can install all licenses at the same time even though you have not yet created all elements that the licenses are bound to.

Steps

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

1) In the Management Client, select **Menu** > **System Tools** > **Install Licenses**.

2) Select one or more license files to install in the dialog box that opens and click **Install**.

3) To check that the licenses were installed correctly, select **Configuration**, then browse to **Administration** > **Licenses** > **All Licenses**.

   One license is shown for each NGFW Engine node. You must bind POL-bound licenses manually to the correct NGFW Engine nodes after you have configured the NGFW Engine elements. POS-bound licenses are automatically bound to the NGFW Engine nodes when you install a policy on the NGFW Engine after the NGFW Engine makes initial contact with the Management Server.

Next steps

Define the engine elements.

Related concepts

Types of licenses for SMC servers and NGFW Engines on page 30
Configuring Single Firewalls on page 78
Configuring Firewall Clusters on page 103

Configuring Single Firewalls

After you have the SMC installed and running, you can configure the Single Firewall elements.

Little configuration is done directly on the engines. Most of the configuration is done using the Management Client. The engines cannot be successfully installed before defining them in the Management Client.

The tasks you must complete are as follows:

1) Add Single Firewall elements.

2) Add interfaces and define their properties.

3) (Optional) Select system communication roles for the interfaces.

4) Bind Management Server POL-bound licenses to specific Single Firewall elements.

Add Single Firewall elements

To add a single-node firewall to the SMC, add a Single Firewall element that stores the configuration information related to the firewall.

Note

You can also create several Single Firewall elements at the same time using the Create Multiple Single Firewalls wizard. For more information about creating several Single Firewall elements at the same time, see the *Forcepoint Next Generation Firewall Product Guide*.

Steps

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

1) Select **Configuration**.

2) Right-click **NGFW Engines**, then select **New** > **Firewall** > **Single Firewall**.

3) In the **Name** field, enter a unique name.

4) From the **Log Server** drop-down list, select the Log Server for storing logs.

5) (Optional) In the **DNS IP Addresses** list, add one or more IP addresses.
   The NGFW Engine uses the DNS servers at these IP addresses to resolve malware signature mirrors, domain names, and web filtering categorization services. There are two ways to define IP addresses:
   - To enter an IP address, select **Add** > **IP Address**, then enter the IP address.
   - To use an element that represents an IP address, select **Add** > **Network Element**, then select a Host or External DNS Server element.

6) (Optional) From the **Location** drop-down list, select the Location to which the NGFW Engine belongs.

7) (Optional) If you have a Forcepoint NGFW appliance, copy and paste the proof-of-serial (POS) code delivered with the appliance to the **Proof-of-Serial** field.
   Using the POS code allows you to configure the Single Firewall engine using plug and play configuration.

8) Click **Save**.
   Do not close the Engine Editor.

Next steps

Add the interfaces.

Related tasks
Prepare for plug-and-play configuration on page 182

Add layer 3 interfaces to Single Firewalls

Layer 3 interfaces are used in system communications and in traffic inspection on Single Firewalls.

Add layer 3 physical interfaces to Single Firewalls

To route traffic through the firewall, you must define at least two layer 3 physical interfaces.

Note

Only the interface that is used for communications between the Management Server and the Firewall is required when you install the Single Firewall. Although you can configure more interfaces at any time, it is recommended to add more interfaces right away.

There are three types of layer 3 physical interfaces:

- An interface that corresponds to a single network interface on the firewall engine. In the Management Client, the interface type is **None**.
- An *aggregated link in high availability mode* represents two interfaces on the firewall engine. Only the first interface in the aggregated link is actively used. The second interface becomes active only if the first interface fails.
  Connect the first interface in the link to one external switch and the second interface to another external switch.
- An *aggregated link in load balancing mode* represents two or more interfaces (up to eight interfaces) on the firewall engine. All interfaces in the aggregated link are actively used and connections are automatically balanced between the interfaces.
  Link aggregation in load-balancing mode is implemented based on the IEEE 802.3ad Link Aggregation standard. Connect all interfaces to a single external switch. Make sure that the switch supports the Link Aggregation Control Protocol (LACP) and that LACP is configured on the switch.

Steps

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

1) In the navigation pane on the left, browse to **Interfaces**.
2) Select **Add** > **Layer 3 Physical Interface**.
3) From the **Interface ID** drop-down list, select an ID number.
   This ID maps to a network interface during the initial configuration of the engine.
4) From the **Type** drop-down list, select the interface type.
5) If the type is aggregated link, select one or more other interfaces that belong to the aggregated link.

- For an aggregated link in high availability mode, select an interface ID from the **Second Interface ID** drop-down list.
- For an aggregated link in load balancing mode, click **Add** to add one or more interface IDs to the **Additional Interface(s)** list.

6) Click **OK**.

7) Click **Save**.
Do not close the Engine Editor.

Result

The layer 3 physical interface is added to the interface list.

Next steps

Add VLAN interfaces or IP addresses to the layer 3 physical interface.

Related tasks
Add VLAN interfaces to layer 3 physical interfaces of Single Firewalls on page 81
Add IP addresses to Single Firewall interfaces on page 87

Add VLAN interfaces to layer 3 physical interfaces of Single Firewalls

VLANs divide a single physical network link into several virtual links.

You can add up to 4094 VLANS to each physical interface.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a physical interface and select **New** > **VLAN Interface**.

3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).

Note

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.

4) Click **OK**.
The specified VLAN ID is added to the physical interface.

5) Click **Save**.
Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Next steps

Continue the configuration in one of the following ways:

- Add IP addresses to the VLAN interfaces.
- Add other types of interfaces.

Related tasks

Add IP addresses to Single Firewall interfaces on page 87

Add wireless interfaces to Single Firewalls

You can add one wireless interface to a Single Firewall.

Wireless interfaces are only supported on specific Forcepoint NGFW appliances that have an integrated wireless network interface card.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click the empty space and select **New** > **Wireless Interface**.

3) From the **Interface ID** drop-down list, select the interface ID number.
This ID number maps to the wireless port during the initial configuration of the engine.

4) In the **Country** field, enter or select the country where the firewall is used as a wireless access point.

5) From the **Band** drop-down list, select the band for the wireless interface access point.

6) From the **Wireless Mode** drop-down list, select the mode for transmitting the wireless traffic according to the capabilities of the connecting clients.

The wireless mode options that you can select depend on the band.

Band	Wireless mode
2.4 GHz	802.11b
	802.11bg
	802.11g
	802.11n
	802.11bgn
5 GHz	802.11a
	802.11an
	802.11n
	802.11ac
	802.11acn

Note

Some wireless clients do not support the 802.11n, 802.11ac, and 802.11acn wireless modes with the WEP security mode.

7) From the **Channel** drop-down list, select the channel for transmitting the wireless traffic.

If there are other wireless access points nearby, use channels that are as far apart as possible to avoid interference. Security Management Center might sometimes select another channel to use the best frequency available. If you select **Automatic**, the best channel is automatically selected.

8) (Optional) From the **Width** drop-down list, select the width of the channel. This option is only available if the Wireless Mode is one of the following: 802.11n, 802.11bgn, 802.11an, 802.11n, 802.11ac, or 802.11acn.

9) (Optional) From the **Transmit Power** drop-down list, select the maximum power of the signal for transmitting the wireless traffic.

- The power options are shown as milliwatts (mW) and as the power ratio in decibels of the measured power referenced to 1 milliwatt (dBm).
- The values available depend on the regulatory limits for the selected country and the channel for the wireless interface.
- If you are not sure what value to use, leave the default value selected.

10) Click **OK**.

The wireless interface is added to the interface list.

11) Click **Save**.

Do not close the Engine Editor.

Next steps

Add SSID interfaces to the wireless interface.

Add SSID interfaces to Single Firewalls

A service set identifier (SSID) interface represents an 802.11 wireless LAN.

You can add several **SSID Interfaces** to the **Wireless Interface**.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click the wireless interface and select **New SSID Interface**.

3) In the **Wireless Network Name (SSID)** field, enter the wireless network name.
It identifies the network to the end users.

4) From the **Wireless SSID Broadcast** drop-down list, select one of the following options:
   - **Enabled** — The wireless network name is broadcast to anyone in range.
   - **Disabled** — Users must type the name to connect.

5) From the **MAC Address Type** drop-down list, select one of the following options:
   - **Hardware** — The first SSID Interface that you define is automatically assigned the MAC address of the wireless card.
   - **Custom** — A custom MAC address.

6) (Custom MAC address only) In the **MAC Address** field, enter a MAC address.

7) Click the **Security** tab.

8) From the **Security Mode** drop-down list, select the security mode.

Tip

When you select the security mode, the options particular for that mode are enabled. We recommend using one of the WPA security modes.

9) If you selected **WEP Open System** or **WEP Shared Key**, configure these options.
   a) From the **Key Length** drop-down list, select the key length.
   b) From the **Default Key** drop-down list, select which key is used by default.
   c) Enter 1–4 encryption keys.

10) If you selected **WPA Personal**, configure these options.
   a) From the **WPA Mode** drop-down list, select the WPA mode.
   b) In the **Pre-Shared Key** field, enter a pre-shared key of 8 to 64 ASCII characters.

11) If you selected **WPA Enterprise**, configure these options.
   a) From the **WPA Mode** drop-down list, select the WPA mode.
   b) Next to the **Authentication Method** field, click **Select**.
   c) Select the RADIUS authentication method for authenticating users and click **Select**.

12) Click **OK**.

13) Click **Save**.
   Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add IP addresses to the SSID Interfaces.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Firewall elements.

Related tasks

Add IP addresses to Single Firewall interfaces on page 87
Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Add Switches to Single Firewalls

An integrated switch represents the switch functionality on purpose-built Forcepoint NGFW appliances. Integrated switches eliminate the need for an external switch device and reduce costs and clutter.

The switch functionality is only supported on specific Forcepoint NGFW appliances that have a hardware or software integrated switch. For more information, see the model-specific *Forcepoint Next Generation Firewall Hardware Guide* for your Forcepoint NGFW appliance.

- On Forcepoint NGFW appliances that have hardware integrated switches, you can configure one integrated switch and one or more port group interfaces.
- On Forcepoint NGFW appliances that have software integrated switches, you can configure one or more integrated switches, and one port group interface on each integrated switch.

You can only use the integrated switch if the appliance has been configured as a Single Firewall.

Note

The ports in the integrated switch do not support VLAN tagging or PPPoE. You cannot use ports on the integrated switch as the control interface.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.
2) Right-click the empty space and select **New** > **Switch**.
3) From the **Switch ID** drop-down list, select the ID according to your switch type. For example, the switch ID of the Forcepoint NGFW 110 appliance is 0. See the *Hardware Guide* for your appliance for more information.
4) From the **Switch Type** drop-down list, select the type of your Forcepoint NGFW switch.
5) Click **OK**.
6) Click **Save**.
   Do not close the Engine Editor.

Next steps

Add port group interfaces to the switch.

Add Port Group Interfaces to Single Firewalls

Port groups simplify port and network segment configuration. Traffic inside a port group is not inspected. The traffic between port groups is inspected by the firewall in the same way as other traffic.

Before you begin

You must add the integrated switch before you can add port group interfaces.

Depending on the Forcepoint NGFW appliance model, you can define one or more port group interfaces and add different types of interfaces to the port group:

- On Forcepoint NGFW appliances that have hardware integrated switches, you can define one or more port group interfaces on the integrated switch.
  You can add physical interfaces to the port group interface.
- On Forcepoint NGFW appliances that have software integrated switches, you can define one port group interface on each integrated switch.
  You can add physical interfaces and SSID interfaces to the port group interface.

For more information about the type of integrated switch that your appliance has, see the model-specific *Forcepoint Next Generation Firewall Hardware Guide* for your Forcepoint NGFW appliance.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.
2) Right-click the switch and select **New Port Group Interface**.
3) Define the port group interface properties.
4) Click **OK**.
   The port group interface is added to the interface list. The defined switches and port group interfaces are displayed, for example, as “0.1” for switch ID 0 with port group 1.
5) Click **Save**.
   Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add IP addresses to the port group interfaces.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Firewall elements.

Related tasks

Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Add IP addresses to Single Firewall interfaces

You can add one or more IP addresses to each interface on a Single Firewall.

The number and types of IP addresses that you can add depend on the interface type.

IP addresses for each interface type

Interface type	Static IPv4 addresses	Dynamic IPv4 Addresses	Static IPv6 Addresses	Dynamic IPv6 Addresses
Physical interface	One or more	One	One or more	One
Aggregated Link interface	One or more	None	One or more	None
VLAN interface	One or more	One	One or more	One

Interface type	Static IPv4 addresses	Dynamic IPv4 Addresses	Static IPv6 Addresses	Dynamic IPv6 Addresses
Port group interface	One or more	One	One or more	One
SSID interface	One	None	One	None

Add static IPv4 addresses to Single Firewall interfaces

Depending on the type of interface, you can add one or more static IPv4 addresses to Single Firewall interfaces.

Steps

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

1) In the navigation pane on the left, browse to **Interfaces**.

2) Right-click a physical interface, VLAN interface, SSID interface, or port group interface, then select **New** > **IPv4 Address**.

3) In the **IPv4 Address** field, enter the IPv4 address.

4) In the **Netmask** field, adjust the automatically added netmask if necessary.
   The Network Address and Broadcast IP address are updated accordingly.

5) If the interface is used for system communications and NAT is applied, add contact addresses.
   a) If the default contact address is not dynamic, deselect **Dynamic** and enter the static contact address.
   b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.

6) If you want to use Virtual Router Redundancy Protocol (VRRP), add a virtual router.

   Note

   One virtual router can be configured for each physical interface, VLAN interface, or port group interface. Although VRRP support is also available, for port group interfaces, it is not normally used.

   a) Click **VRRP Settings**.
   b) Select **Enable VRRP**.
   c) Fill in the **ID**, **Priority**, and **IPv4 Address** fields according to the configuration of the virtual router.

d) Click **OK**.

7) Click **OK**.
The IPv4 address is added to the interface.

8) Click **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add more IP addresses.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Firewall elements.

Related tasks
Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Add static IPv6 addresses to Single Firewall interfaces

Depending on the type of interface, you can add one or more static IPv6 addresses to Single Firewall interfaces.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a physical, VLAN, SSID, or port group interface and select **New** > **IPv6 Address**.

3) In the **IPv6 Address** field, enter the IPv6 address.

Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

4) Enter the Prefix Length (0–128).

5) Click **OK**.

6) Click **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add more IP addresses.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Firewall elements.

Related tasks

Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Add dynamic IPv4 addresses to Single Firewall interfaces

You can configure dynamic IPv4 addresses for physical, VLAN, ADSL, and port group interfaces on Single Firewalls.

Note

Dynamic IP addresses are not supported on Aggregated Link interfaces.

You can identify interfaces that have a dynamic IPv4 address using a DHCP Index. A modem interface always has a dynamic IP address.

Steps

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

1) In the navigation pane on the left, browse to **Interfaces**.
2) Right-click a physical, VLAN, ADSL, or port group interface, then select **New** > **IPv4 Address**.
3) Select **Dynamic** as the type of IP address.
4) From the **Dynamic Index** drop-down list, select a DHCP index.
   The index is used for identification in other parts of the configuration (such as Firewall Policies) to represent the possibly changing IP address.
5) If the interface is used for system communications and NAT is applied, add contact addresses.
   a) If the default contact address is not dynamic, deselect **Dynamic**, then enter the static contact address.
   b) If components from some locations must use a different IP address for contact, click **Exceptions**, then define the location-specific addresses.

6) If the interface's dynamic IP address is assigned through point-to-point protocol, configure the settings.
PPPoE can be used with physical, VLAN or ADSL interfaces. PPPoA can be used with ADSL interfaces only.
   a) Click **PPP Settings**.
   b) From the **Mode** drop-down list, select **PPPoE**.
   c) Fill in the **User Name**, **Password**, and (optional) **Service Name** fields according to the details provided by your service provider.
   If you do not have these details, contact your service provider. By default, passwords and keys are not shown in plain text. To show the password or key, deselect the **Hide** option.
   d) Click **OK**.

7) Click **OK**.
The dynamic IPv4 address is added to the interface.

8) Click **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add more IP addresses.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Firewall elements.

Related tasks
Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Add dynamic IPv6 addresses to Single Firewall interfaces

You can add dynamic IPv6 addresses to physical interfaces, VLAN interfaces, and port group interfaces on Single Firewalls.

Note
Dynamic IP addresses are not supported on Aggregated Link interfaces.

You can identify interfaces that have a dynamic IPv6 address using a DHCP Index.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a physical interface and select **New** > **IPv6 Address**.

3) In the **IP Address Properties** dialog box, select **Dynamic**.

4) From the **Dynamic Index** drop-down list, select a DHCP index.
   The index is used for identification in other parts of the configuration (such as IPS Policies) to represent the possibly changing IP address.

5) If the interface is used for system communications and NAT is applied, add contact addresses.
   a) Enter the default contact address in one of the following ways:
      - In the **Default** field, enter the contact address.
      - Select **Dynamic** and define the translated IP address of this component.

   b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.

6) (Optional) If you do not want a default route to be automatically created through the interface, deselect **Automatic Default Route**.

7) (Optional) If you want to use DHCPv6 to get the IPv6 address, select **Use DHCPv6 to get IPv6 Address**.

8) Click **OK**.
   The IP address is added to the interface.

9) Click **Save**.
   Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add more IP addresses.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Firewall elements.

Related tasks

Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Add modem interfaces to Single Firewalls

You can use mobile broadband modems with Single Firewalls to provide wireless links for outbound connections.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click the empty space, then select **New** > **Modem Interface**.

3) From the **Modem Type** drop-down list, select the type of mobile broadband modem that was delivered with your appliance.

4) From the **Modem Number** drop-down list, select the modem number that is mapped to the modem's IMEI (international mobile equipment identity) number.

5) From the **DHCP index** drop-down list, select the DHCP index number.
The DHCP index is a number for your own reference to identify the DHCP interface.

6) In the **PIN** field, enter the PIN code if it is needed for the modem's SIM card.

7) Fill in the **Access Point Name** field according to the instructions that you have received from your service provider.

8) (3G Modem only) In the **Phone Number** field, enter the modem's phone number if it differs from the default phone number.

9) (3G Modem only) Fill in the **Service Name** fields according to the instructions that you have received from your service provider.

10) (LTE Modem only) If the service provider requires authentication, select the authentication method from the **Auth Method** drop-down list according to the instructions that you have received from your service provider.

11) (3G Modem or when an authentication method is selected) Fill in the **Username** and **Password** fields according to the instructions that you have received from your service provider.

12) If necessary, define the contact address information.
If components from some Locations cannot use the Default contact address, click **Exceptions** to define Location-specific contact addresses.

13) Click **OK**.
The Modem Interface is added to the interface list.

14) Click **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Firewall elements.

Related tasks

Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Add layer 2 interfaces to Single Firewalls

Layer 2 interfaces are used in traffic inspection on Single Firewalls.

Add logical interfaces to Single Firewalls

Logical Interface elements are used in the Layer 2 Interface Policy and the traffic inspection process to represent a network segment.

The SMC contains one default Logical Interface element. A logical interface can represent any number or combination of physical interfaces and VLAN interfaces. However, the same logical interface cannot be used to represent both inline IPS interfaces and inline Layer 2 Firewall interfaces on the same Single Firewall. The rules in the ready-made Layer 2 Interface Template policy match all logical interfaces.

Steps

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

1) Select **Configuration**.

2) Expand the **Other Elements** branch.

3) Right-click **Logical Interfaces** and select **New Logical Interface**.

4) In the **Name** field, enter a unique name.

5) (Optional) If you use VLAN tagging, select **View interface as one LAN**.
   By default, the Single Firewall treats a single connection as multiple connections when an external switch passes traffic between different VLANs and all traffic is mirrored to the Single Firewall through a SPAN port.

6) Click **OK**.
   Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- If you want to use reset interfaces with capture interfaces, add reset interfaces.

- Add capture interfaces or inline interfaces.

Related tasks

Add reset interfaces to Single Firewalls on page 95
Add capture interfaces to Single Firewalls on page 96
Add inline IPS interfaces to Single Firewalls on page 97
Add inline Layer 2 Firewall interfaces to Single Firewalls on page 99

Add reset interfaces to Single Firewalls

Reset interfaces can deliver TCP resets and ICMP destination unreachable messages to interrupt communications picked up from capture interfaces when the communications trigger a response.

VLANs are supported for sending resets, but the correct VLAN is selected automatically. An interface you want to use as the reset interface must not have any manually added VLAN configuration.

The reset interface must be in the same broadcast domain as the capture interface that uses the reset interface. The resets are sent using the IP addresses and MAC addresses of the communicating hosts.

Important

An interface that is used only as a reset interface must not have an IP address.

Steps

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

1) Right-click the Single Firewall and select **Edit <element type>**.
   The Engine Editor opens.
2) In the navigation pane on the left, browse to **Interfaces**.
3) Right-click the empty space and select **New Layer 3 Physical Interface**.
4) From the **Interface ID** drop-down list, select an ID number.
5) From the **Type** drop-down list, select **None**.
6) Click **OK**.
7) Click **Save**.
   Do not close the Engine Editor.

Result

This interface can now be used as a reset interface. When you set up the physical network, make sure that the reset interface connects to the same network as the capture interfaces.

Next steps

Add capture interfaces.

Add capture interfaces to Single Firewalls

Capture interfaces monitor traffic that external devices have duplicated for inspection to the Single Firewall.

You can have as many capture interfaces as there are available physical ports on the Single Firewall (there are no license restrictions regarding this interface type).

External equipment must be set up to mirror traffic to the capture interface. You can connect a capture interface to an external switch SPAN port or a network TAP to capture traffic.

Steps

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

1) Right-click the Single Firewall and select **Edit <element type>**.
   The Engine Editor opens.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click the empty space and select **New Layer 2 Physical Interface**.

4) From the **Interface ID** drop-down list, select an ID number.

5) From the **Type** drop-down list, select **Capture Interface**.

6) (Optional) From the **Reset Interface** drop-down list, select a TCP reset interface for traffic picked up through this capture interface.

7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
   - Select an existing Logical Interface element from the list.
   - Click **Select** and browse to another Logical Interface element.
   - Click **New** to create a Logical Interface element, then click **OK**.

8) If you want the Single Firewall to inspect traffic from VLANs that are not included in the Single Firewall's interface configuration, leave **Inspect Unspecified VLANs** selected.

9) If you want the Single Firewall to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.

10) Click **OK**.

11) Click **Save**.
    Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLAN interfaces to the capture interface.
- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.

- Bind engine licenses to the Single Firewall elements.

Related tasks

Add VLAN interfaces to layer 2 interfaces of Single Firewalls on page 100
Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Add inline IPS interfaces to Single Firewalls

There are two physical interfaces in an inline IPS interface. The traffic is forwarded from one interface to the other.

The traffic that the Single Firewall allows goes through the inline IPS interface as if it was going through a network cable. The Single Firewall drops the traffic you want to stop.

Inline interfaces are associated with a Logical interface element. The Logical interface is used in the Layer 2 Interface Firewall Policies and the traffic inspection process to represent one or more inline IPS interfaces.

Fail-open network cards have fixed pairs of ports. Make sure to map these ports correctly during the initial configuration of the engine. If you use the automatic USB memory stick configuration method for the engine's initial configuration, the ports are configured automatically.

Steps

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

1) Right-click the Single Firewall engine and select **Edit <element type>**.
   The Engine Editor opens.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click the empty space and select **New Layer 2 Physical Interface**.

4) From the **Interface ID** drop-down list, select an ID number.

5) From the **Type** drop-down list, select **Inline IPS Interface**.

6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.

7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
   - Select an existing Logical Interface element from the list.
   - Click **Select** and browse to another Logical Interface element.
   - Click **New** to create a Logical Interface element, then click **OK**.

8) If you want the Single Firewall to inspect traffic from VLANs that are not included in the Single Firewall's interface configuration, leave **Inspect Unspecified VLANs** selected.

9) If you want the Single Firewall to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.

10) Click **OK**.

11) Click **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Define how the Single Firewall handles traffic when the traffic load is too high using the **Bypass Traffic on Overload** setting.
- Add VLAN interfaces to the inline IPS interface.
- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Firewall elements.

Related tasks

Bypass traffic on overload on Single Firewalls on page 98
Add VLAN interfaces to layer 2 interfaces of Single Firewalls on page 100
Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Bypass traffic on overload on Single Firewalls

You can configure the Single Firewall to bypass traffic when the traffic load becomes too high.

By default, Single Firewalls inspect all connections. If the traffic load is too high for the Single Firewall to inspect all connections, the Single Firewall can dynamically reduce the number of inspected connections. This reduction can improve performance in evaluation environments, but some traffic might pass through without any access control or inspection.

CAUTION

Using bypass mode requires a fail-open network interface card. If the ports that represent the interfaces cannot fail open, policy installation fails on the engine. Bypass mode is not compatible with VLAN retagging. In network environments where VLAN retagging is used, normal mode is automatically enforced.

Steps

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

1) Right-click the Single Firewall engine and select **Edit <element type>**.
The Engine Editor opens.

2) In the navigation pane on the left, select **General** > **Layer 2 Settings**.

3) Select **Bypass Traffic on Overload**.

4) Click **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to Single Firewall elements.

Related tasks

Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Add inline Layer 2 Firewall interfaces to Single Firewalls

There are two physical interfaces in an inline Layer 2 Firewall interface. The traffic is forwarded from one interface to the other.

The traffic that the Single Firewall allows goes through the inline Layer 2 Firewall interface as if it was going through a network cable. The Single Firewall drops the traffic you want to stop. If the Single Firewall is unable to process traffic, all traffic that goes through the inline Layer 2 Firewall interface is blocked.

Inline interfaces are associated with a Logical interface element. The Logical interface is used in the Layer 2 Interface Firewall Policies and the traffic inspection process to represent one or more inline Layer 2 Firewall interfaces.

Steps

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

1) Right-click the Single Firewall engine and select **Edit <element type>**.
   The Engine Editor opens.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click the empty space and select **New Layer 2 Physical Interface**.

4) From the **Interface ID** drop-down list, select an ID number.

5) From the **Type** drop-down list, select **Inline Layer 2 Firewall Interface**.

6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.

7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
   - Select an existing Logical Interface element from the list.
   - Click **Select** and browse to another Logical Interface element.
   - Click **New** to create a Logical Interface element, then click **OK**.

8) If you want the Single Firewall to inspect traffic from VLANs that are not included in the Single Firewall's interface configuration, leave **Inspect Unspecified VLANs** selected.

9) If you want the Single Firewall engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.

10) Click **OK**.

11) Click **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLAN interfaces to the inline Layer 2 Firewall interface.
- Select system communication roles for interfaces.
- Bind engine licenses to Single Firewall elements.

Related tasks

Add VLAN interfaces to layer 2 interfaces of Single Firewalls on page 100
Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Add VLAN interfaces to layer 2 interfaces of Single Firewalls

VLANs divide a single physical network link into several virtual links.

You can add up to 4094 VLANS to each physical interface.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a physical interface and select **New** > **VLAN Interface**.

3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).

Note

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.

4) Click **OK**.
The specified VLAN ID is added to the physical interface.

5) Click **Save**.
Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Next steps

Continue the configuration in one of the following ways:

- Select system communication roles for interfaces.
- Bind engine licenses to Single Firewall elements.

Related tasks
Select system communication roles for Single Firewall interfaces on page 101
Bind engine licenses to Single Firewall elements on page 102

Select system communication roles for Single Firewall interfaces

Select which IP addresses are used for particular roles in system communications.

For example, you can select which IP addresses are used in communications between the Firewall and the Management Server.

The interfaces you have defined are shown as a tree-table on the Interfaces tab. Global interface options have codes in the tree-table.

Interface option codes

Code	Description
A	The interface that has the IP address used as the identity for authentication requests.
C	The interface that have the primary and backup control IP addresses.
O	The default IP address for outgoing connections.

Note

You cannot use layer 2 physical interfaces on firewalls for system communications.

Steps

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

1) In the navigation pane on the left, select **Interfaces** > **Interface Options**.

2) Select the interface options.

   a) From the **Primary** drop-down list, select the primary control IP address that the Firewall uses for communications with the Management Server.

   b) (Optional, recommended) From the **Backup** drop-down list, select a backup control IP address that the Firewall uses for communications with the Management Server if the primary control IP address fails.

   c) If the Firewall's primary control IP address and backup control IP address are dynamic or if the Firewall is in an environment where only the Firewall can initiate connections to the Management Server, select **Node-initiated contact to Management Server**.

   When this option is selected, the engine opens a connection to the Management Server and maintains connectivity.

   d) From the **Identity for Authentication Requests** drop-down list, select the IP address that identifies the firewall to external authentication servers.

   Note

   This selection has no effect on routing.

   e) (Optional) From the **Source for Authentication Requests** drop-down list, select the IP address that identifies the firewall when it sends an authentication request to an external authentication server over a VPN.

   Note

   This selection has no effect on routing.

   f) From the **Default IP Address for Outgoing Traffic** drop-down list, select the IP address that nodes use if they have to initiate connections through an interface that has no Node Dedicated IP address.

3) Click **Save**, then close the Engine Editor.

Next steps

Bind engine licenses to the Single Firewall elements.

Bind engine licenses to Single Firewall elements

After you have configured the Single Firewall elements, you must manually bind Management Server POL-bound licenses to specific Single Firewall elements.

Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. POS-bound appliance licenses are automatically bound to the correct Firewall element when the engine is fully installed.

Steps

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

1) Select **Configuration**, then browse to **Administration**.
2) Browse to **Licenses** > **Engine** or **Licenses** > **Firewall** depending on the type of licenses you have.
   All installed licenses appear in the right pane.
3) Right-click a Management Server POL-bound license and select **Bind**.
4) Select the node and click **Select**.
   The license is now bound to the selected Firewall element.

Tip

If you bound the license to an incorrect element, right-click the license and select **Unbind**.

CAUTION

When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently bound licenses can't be rebound to another engine without relicensing or deleting the engine element the license is bound to. Until you do that, the unbound license is shown as Retained.

Next steps

Transfer the configuration to the Firewall engines.

Related concepts

Options for initial configuration on page 181

Configuring Firewall Clusters

After you have the SMC installed and running, you can configure the Firewall Cluster elements.

Little configuration is done directly on the engines. Most of the configuration is done using the Management Client. The engines cannot be successfully installed before defining them in the Management Client.

The tasks you must complete are as follows:

1) Add Firewall Cluster elements.
2) Add the necessary number of nodes to the Firewall Cluster.
3) Add interfaces and define their properties.
4) (Optional) Select system communication roles for the interfaces.
5) Bind Management Server POL-bound licenses to specific nodes in the Firewall Cluster.

Operating modes for Firewall Cluster interfaces

There are several operating modes for the physical interfaces of a Firewall Cluster. Packet dispatch mode is recommended for new installations.

The other modes are provided for backward compatibility. See the *Forcepoint Next Generation Firewall Product Guide* for more information about the other operating modes.

In packet dispatch mode:

- There is only one contact MAC address for each physical interface. The dispatcher node controls this MAC address.
- The dispatcher node forwards the packets to the other nodes for processing. Any node in the cluster can process the traffic.
- The dispatcher node is chosen separately for each physical interface.

Note

Different nodes might be selected as dispatcher nodes for different physical interfaces.

The packet dispatcher for the physical interface changes automatically if the dispatcher goes offline. When the dispatcher changes:

- The packet dispatcher MAC address is moved to another firewall node.
- The firewall sends an ARP message to the external switch or router.
- The switch or router updates its address table.

Note

This process is a standard network addressing operation where the switch or router learns that the MAC address is located behind a different port.

- The switch or router forwards traffic destined to the physical interface to this new packet dispatcher.

Add Firewall Cluster elements

To introduce a new Firewall Cluster to the SMC, you must define a Firewall Cluster element that stores the configuration information related to the Firewalls.

Steps

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

1) Select **Configuration**.

2) Right-click **NGFW Engines**, then select **New** > **Firewall** > **Firewall Cluster**.

3) In the **Name** field, enter a unique name.

4) From the **Log Server** drop-down list, select the Log Server for storing logs.

5) (Optional) In the **DNS IP Addresses** list, add one or more IP addresses.

   The NGFW Engine uses the DNS servers at these IP addresses to resolve malware signature mirrors, domain names, and web filtering categorization services. There are two ways to define IP addresses:

- To enter an IP address, select **Add** > **IP Address**, then enter the IP address.
- To use an element that represents an IP address, select **Add** > **Network Element**, then select a Host or External DNS Server element.

6) (Optional) From the **Location** drop-down list, select the Location to which the NGFW Engine belongs.

7) Click **Save**.
Do not close the Engine Editor.

Add nodes to Firewall Clusters

The Firewall Cluster element has two nodes when the element is created.

Firewall Clusters can have up to 16 nodes. Add all nodes you plan to install before you begin configuring the interfaces.

Steps

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

1) In the navigation pane on the left, select **General** > **Clustering**.

2) (Optional) In the **Name** field, change the name.

3) Click **OK**.
The node is added to the Firewall Cluster.

4) Click **Save**.
Do not close the Engine Editor.

Add layer 3 interfaces to Firewall Clusters

Layer 3 interfaces are used in system communications and in traffic inspection on Firewall Clusters.

Add layer 3 physical interfaces to Firewall Clusters

To route traffic through the Firewall Cluster, you must define at least two layer 3 physical interfaces.

We recommend defining at least two interfaces for the Firewall Cluster:

- An interface used for communications between the Management Server and the Firewall.
- An interface for the heartbeat communications between the cluster nodes. The heartbeat traffic is critical to the functioning of the cluster, so it is highly recommended to have a dedicated heartbeat interface.

Although you can configure more interfaces at any later time, it is simplest to add more interfaces right away. This action allows traffic to be routed through the Firewall. You can use the Cluster installation worksheet to document the interfaces.

There are three types of layer 3 physical interfaces on Firewall Clusters:

- An interface that corresponds to a single network interface on each node in the Firewall Cluster. In the Management Client, the interface type is **None**.
- An *aggregated link in high availability mode* represents two interfaces on each node. Only the first interface in the aggregated link is actively used. The second interface becomes active only if the first interface fails. Connect the first interface in the link to one external switch and the second interface to another external switch.
- An *aggregated link in load balancing mode* represents two or more interfaces (up to eight interfaces) on each node. All interfaces in the aggregated link are actively used and connections are automatically balanced between the interfaces.
  Link aggregation in load-balancing mode is implemented based on the IEEE 802.3ad Link Aggregation standard. Connect all interfaces to a single external switch. Make sure that the switch supports the Link Aggregation Control Protocol (LACP) and that LACP is configured on the switch.

Steps

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

1) In the navigation pane on the left, browse to **Interfaces**.

2) Select **Add** > **Layer 3 Physical Interface**.

3) From the **Interface ID** drop-down list, select an interface ID number.
   This ID maps to a network interface during the initial configuration of the engine.

4) From the **Type** drop-down list, select the interface type.

5) If the type is **Aggregated Link**, select one or more other interfaces that belong to the aggregated link.
   - For an aggregated link in high availability mode, select an interface ID from the **Second Interface ID** drop-down list.
   - For an aggregated link in load balancing mode, click **Add** to add one or more interface IDs to the **Additional Interface(s)** list.

6) Leave **Packet Dispatch** selected as the CVI Mode, then enter a MAC Address with an even number as the first octet.

   Important

   This MAC address must not belong to any actual network card on any of the nodes.

   - Packet Dispatch is the primary clustering mode in new installations.
   - Different CVI modes can be used for different interfaces of a Firewall Cluster without limitations.

   Note

   All CVI addresses that are defined for the same physical interface must use the same unicast MAC address. The dispatcher nodes use the MAC address you define here. Other nodes use their network card's MAC address.

7) (Optional) In the **MTU** field, enter the MTU value if this link requires a lower MTU than the Ethernet-default 1500.

8) Click **OK**.

9) Click **Save**.
Do not close the Engine Editor.

Result

The layer 3 physical interface is added to the interface list.

Next steps

Add VLAN interfaces or IP addresses to the layer 3 physical Interface.

Related tasks
Add VLAN interfaces to layer 3 interfaces of Firewall Clusters on page 107
Add IP addresses to Firewall Cluster interfaces on page 108

Add VLAN interfaces to layer 3 interfaces of Firewall Clusters

VLANs divide a single physical network link into several virtual links.

You can add up to 4094 VLANs to each physical interface.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a physical interface and select **New** > **VLAN Interface**.

3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).

Note

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.

4) Click **OK**.
The specified VLAN ID is added to the physical interface.

5) Click **Save**.
Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Next steps

Continue the configuration in one of the following ways:

- Add IP addresses to the VLAN interfaces.
- Add other types of interfaces.

Add IP addresses to Firewall Cluster interfaces

To route traffic through the firewall, each Firewall Cluster interface must have at least two IP addresses.

Firewall Clusters can have two types of IP addresses.

Types of IP addresses for Firewall Clusters

Interface type	Description	When to use it
Cluster Virtual IP address (CVI)	An IP address that is used to handle traffic routed through the cluster for inspection. All nodes in a cluster share this IP address. Allows other devices to communicate with the Firewall Cluster as a single entity.	Define a CVI for the interface if traffic that the firewall inspects is routed to or from the interface.
Node Dedicated IP address (NDI)	An IP address that is used for traffic to or from an individual node in a cluster. Each node in the cluster has a specific IP address that is used as the NDI. Used for the heartbeat connections between the engines in a cluster, for control connections from the Management Server, and other traffic to or from individual nodes.	Define at least two NDIs: one for management connections and one for the heartbeat traffic between the nodes. We recommend that you define an NDI for each interface that has a CVI, if practical. Some features might not work reliably without an NDI.

You can define several CVIs and NDIs on the same physical interface or VLAN interface. A physical interface or a VLAN interface can have only a CVI or only an NDI.

IPv6 addresses are supported on Firewall Clusters with dispatch clustering mode. IPv6 and IPv4 addresses can be used together on the same Firewall Cluster.

Add IPv4 addresses to Firewall Cluster interfaces

Add an IPv4 address to a Firewall Cluster interface.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a physical interface or VLAN interface and select **New** > **IPv4 Address**.

3) Select the types of IP addresses that you want to add using the **Cluster Virtual IP Address** and **Node Dedicated IP Address** options.

   By default, both are selected. If the interface does not receive or send traffic that the Firewall examines, there is no need to define a Cluster Virtual IP address (CVI). We recommend adding a Node Dedicated IP address (NDI) for each network or subnetwork that is located behind the physical interface.

4) To add a CVI, enter the IP address in the **IPv4 Address** field in the **Cluster Virtual IP Address** section.

   Tip

   To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

5) If the CVI is used for system communications and NAT is applied, define a contact address for the CVI.

   a) Enter the default contact address in one of the following ways:

   - In the **Default** field, enter the contact address.
   - Select **Dynamic** and define the translated IP address of this component.

   b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.

6) To add NDIs for the nodes, enter the IP address in the **IPv4 Address** field for each node in the **Node Dedicated IP Address** table.

   Tip

   To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

7) If the NDIs are used for system communications and NAT is applied, define a contact address for the NDIs.

   a) Double-click the node's **Contact Address** cell.

   b) In the **Default** field, enter the contact address.

c) (Optional) If components from some locations must use a different IP address for contact, click **Add** and define the location-specific addresses.

d) Click **OK**.

8) (Optional) In the **Netmask** field, change the automatically added netmask if necessary.

9) Click **OK**.
The IPv4 addresses are added to the interface.

10) Click **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add other IP addresses.
- Select system communication roles for interfaces.
- Bind engine licenses to the Firewall Cluster elements.

Related tasks
Select system communication roles for Firewall Cluster interfaces on page 118
Bind engine licenses to Firewall Cluster elements on page 121

Add IPv6 addresses to Firewall Cluster interfaces

Add an IPv6 address for a Firewall Cluster interface.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a physical interface or a VLAN interface and select **New** > **IPv6 Address**.

3) Select the types of IP addresses that you want to add using the **Cluster Virtual IP Address** and **Node Dedicated IP Address** options.
By default, both are selected.
   - If the interface does not receive or send traffic that the firewall examines, there is no need to define a Cluster Virtual IP address.
   - We recommend that you add a Node Dedicated IP address for each (sub)network that is located behind the Physical Interface.

4) If you are adding a Cluster Virtual IP address, in the **IPv6 Address** field, enter the IP address that is used as the Cluster Virtual IP address.

Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

5) If you are adding a Node Dedicated IP address for the nodes, double-click the **IPv6 Address** cell for each node and enter the IP address.

Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

6) (Optional) In the **Prefix Length** field, change the automatically filled in prefix length (0-128).

7) Click **OK**.

8) Click **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add other IP addresses.
- Select system communication roles for interfaces.
- Bind engine licenses to the Firewall Cluster elements.

Related tasks

Select system communication roles for Firewall Cluster interfaces on page 118
Bind engine licenses to Firewall Cluster elements on page 121

Add layer 2 interfaces to Firewall Clusters

Layer 2 interfaces are used in traffic inspection on Firewall Clusters.

Add logical interfaces to Firewall Clusters

Logical Interface elements are used in the Layer 2 Interface Policy and the traffic inspection process to represent a network segment.

The SMC contains one default Logical Interface element. A logical interface can represent any number or combination of physical interfaces and VLAN interfaces. However, the same logical interface cannot be used to represent both inline IPS interfaces and inline Layer 2 Firewall interfaces on the same Firewall Cluster. The rules in the ready-made Layer 2 Interface Template policy match all logical interfaces.

Steps

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

1) Select **Configuration**.
2) Expand the **Other Elements** branch.
3) Right-click **Logical Interfaces** and select **New Logical Interface**.
4) In the **Name** field, enter a unique name.
5) (Optional) If you use VLAN tagging, select **View interface as one LAN**.
   By default, the Firewall Cluster treats a single connection as multiple connections when an external switch passes traffic between different VLANs and all traffic is mirrored to the Firewall Cluster through a SPAN port.
6) Click **OK**.
   Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- If you want to use reset interfaces with capture interfaces, add reset interfaces.
- Add capture interfaces or inline interfaces.

Related tasks

Add reset interfaces to Firewall Clusters on page 112
Add capture interfaces to Firewall Clusters on page 113
Add inline IPS interfaces to Firewall Clusters on page 114

Add reset interfaces to Firewall Clusters

Reset interfaces can deliver TCP resets and ICMP destination unreachable messages to interrupt communications picked up from capture interfaces when the communications trigger a response.

VLANs are supported for sending resets, but the correct VLAN is selected automatically. An interface you want to use as the reset interface must not have any manually added VLAN configuration.

The reset interface must be in the same broadcast domain as the capture interface that uses the reset interface. The resets are sent using the IP addresses and MAC addresses of the communicating hosts.

Important

An interface that is used only as a reset interface must not have an IP address.

Steps

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

1) Right-click the Firewall Cluster and select **Edit <element type>**.
   The Engine Editor opens.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click the empty space and select **New Layer 3 Physical Interface**.

4) From the **Interface ID** drop-down list, select an ID number.

5) From the **Type** drop-down list, select **None**.

6) Click **OK**.

7) Click **Save**.
Do not close the Engine Editor.

Result

This interface can now be used as a reset interface. When you set up the physical network, make sure that the reset interface connects to the same network as the capture interfaces.

Next steps

Add capture interfaces.

Add capture interfaces to Firewall Clusters

Capture interfaces monitor traffic that external devices have duplicated for inspection to the Firewall Cluster.

You can have as many capture interfaces as there are available physical ports on the Firewall Cluster (there are no license restrictions regarding this interface type).

External equipment must be set up to mirror traffic to the capture interface. You can connect a capture interface to an external switch SPAN port or a network TAP to capture traffic.

Steps

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

1) Right-click the Firewall Cluster and select **Edit <element type>**.
The Engine Editor opens.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click the empty space and select **New Layer 2 Physical Interface**.

4) From the **Interface ID** drop-down list, select an ID number.

5) From the **Type** drop-down list, select **Capture Interface**.

6) (Optional) From the **Reset Interface** drop-down list, select a TCP reset interface for traffic picked up through this capture interface.

7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:

- Select an existing Logical Interface element from the list.
- Click **Select** and browse to another Logical Interface element.
- Click **New** to create a Logical Interface element, then click **OK**.

8) If you want the Firewall Cluster to inspect traffic from VLANs that are not included in the Firewall Cluster's interface configuration, leave **Inspect Unspecified VLANs** selected.

9) If you want the Firewall Cluster to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.

10) Click **OK**.

11) Click **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLAN interfaces to the capture interface.
- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Firewall Cluster elements.

Related tasks
Add VLAN interfaces to layer 2 interfaces of Firewall Clusters on page 118
Select system communication roles for Firewall Cluster interfaces on page 118
Bind engine licenses to Single Firewall elements on page 102

Add inline IPS interfaces to Firewall Clusters

There are two physical interfaces in an inline IPS interface. The traffic is forwarded from one interface to the other.

The traffic that the Firewall Cluster allows goes through the inline IPS interface as if it was going through a network cable. The Firewall Cluster drops the traffic you want to stop.

Inline interfaces are associated with a Logical interface element. The Logical interface is used in the Layer 2 Interface Firewall Policies and the traffic inspection process to represent one or more inline IPS interfaces.

Fail-open network cards have fixed pairs of ports. Make sure to map these ports correctly during the initial configuration of the engine. If you use the automatic USB memory stick configuration method for the engine's initial configuration, the ports are configured automatically.

Steps

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

1) Right-click the Firewall Cluster engine and select **Edit <element type>**.
The Engine Editor opens.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click the empty space and select **New Layer 2 Physical Interface**.

4) From the **Interface ID** drop-down list, select an ID number.

5) From the **Type** drop-down list, select **Inline IPS Interface**.

6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.

7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
   - Select an existing Logical Interface element from the list.
   - Click **Select** and browse to another Logical Interface element.
   - Click **New** to create a Logical Interface element, then click **OK**.

8) If you want the Firewall Cluster to inspect traffic from VLANs that are not included in the Firewall Cluster's interface configuration, leave **Inspect Unspecified VLANs** selected.

9) If you want the Firewall Cluster to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.

10) Click **OK**.

11) Click **Save**.
    Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Define how the Firewall Cluster handles traffic when the traffic load is too high using the **Bypass Traffic on Overload** setting.
- Add VLAN interfaces to the inline IPS interface.
- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Firewall Cluster elements.

Related tasks

Bypass traffic on overload on Firewall Clusters on page 115
Add VLAN interfaces to layer 2 interfaces of Firewall Clusters on page 118
Select system communication roles for Firewall Cluster interfaces on page 118
Bind engine licenses to Firewall Cluster elements on page 121

Bypass traffic on overload on Firewall Clusters

You can configure the Firewall Cluster to bypass traffic when the traffic load becomes too high.

By default, Firewall Clusters inspect all connections. If the traffic load is too high for the Firewall Cluster to inspect all connections, the Firewall Cluster can dynamically reduce the number of inspected connections. This reduction can improve performance in evaluation environments, but some traffic might pass through without any access control or inspection.

CAUTION

Using bypass mode requires a fail-open network interface card. If the ports that represent the interfaces cannot fail open, policy installation fails on the engine. Bypass mode is not compatible with VLAN retagging. In network environments where VLAN retagging is used, normal mode is automatically enforced.

Steps

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

1) Right-click the Firewall Cluster and select **Edit <element type>**.
   The Engine Editor opens.

2) In the navigation pane on the left, select **General** > **Layer 2 Settings**.

3) Select **Bypass Traffic on Overload**.

4) Click **Save**.
   Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to Firewall Cluster elements.

Related tasks

Select system communication roles for Firewall Cluster interfaces on page 118
Bind engine licenses to Firewall Cluster elements on page 121

Add inline Layer 2 Firewall interfaces to Firewall Clusters

There are two physical interfaces in an inline Layer 2 Firewall interface. The traffic is forwarded from one interface to the other.

The traffic that the Firewall Cluster allows goes through the inline Layer 2 Firewall interface as if it was going through a network cable. The Firewall Cluster drops the traffic you want to stop. If the Firewall Cluster is unable to process traffic, all traffic that goes through the inline Layer 2 Firewall interface is blocked.

Inline interfaces are associated with a Logical interface element. The Logical interface is used in the Layer 2 Interface Firewall Policies and the traffic inspection process to represent one or more inline Layer 2 Firewall interfaces.

Steps

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

1) Right-click the Firewall Cluster and select **Edit <element type>**.
   The Engine Editor opens.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click the empty space and select **New Layer 2 Physical Interface**.

4) From the **Interface ID** drop-down list, select an ID number.

5) From the **Type** drop-down list, select **Inline Layer 2 Firewall Interface**.

6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.

7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
   - Select an existing Logical Interface element from the list.
   - Click **Select** and browse to another Logical Interface element.
   - Click **New** to create a Logical Interface element, then click **OK**.

8) If you want the Firewall Cluster to inspect traffic from VLANs that are not included in the Firewall Cluster's interface configuration, leave **Inspect Unspecified VLANs** selected.

9) If you want the Firewall Cluster to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.

10) Click **OK**.

11) Click **Save**.
    Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLAN interfaces to the inline Layer 2 Firewall interface.
- Select system communication roles for interfaces.
- Bind engine licenses to Firewall Cluster elements.

Related tasks

Add VLAN interfaces to layer 2 interfaces of Firewall Clusters on page 118
Select system communication roles for Firewall Cluster interfaces on page 118
Bind engine licenses to Firewall Cluster elements on page 121

Add VLAN interfaces to layer 2 interfaces of Firewall Clusters

VLANs divide a single physical network link into several virtual links.

Steps

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a physical interface and select **New** > **VLAN Interface**.

3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).

Note

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.

4) Click **OK**.
The specified VLAN ID is added to the physical interface.

5) Click **Save**.
Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Next steps

Continue the configuration in one of the following ways:

- Select system communication roles for interfaces.
- Bind engine licenses to Firewall Cluster elements.

Related tasks

Select system communication roles for Firewall Cluster interfaces on page 118
Bind engine licenses to Firewall Cluster elements on page 121

Select system communication roles for Firewall Cluster interfaces

Select which IP addresses are used for particular roles in system communications.

For example, you can select which IP addresses are used in communications between the Firewall Cluster and the Management Server.

The interfaces you have defined are shown as a tree-table on the Interfaces tab. Global interface options have codes in the tree-table.

Interface option codes

Code	Description
A	The interface that has the IP address used as the identity for authentication requests.
C	The interfaces that have the primary and backup control IP addresses.
H	The primary and backup heartbeat Interfaces.
O	The default IP address for outgoing connections.

Steps

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

1) In the navigation pane on the left, select **Interfaces** > **Interface Options**.

2) Select the interface options.

   a) From the **Primary** control IP address drop-down list, select the primary control IP address that the Firewall Cluster uses for communications with the Management Server.

   b) (Optional, recommended) In the **Backup** control IP address drop-down list, select a backup control IP address that the Firewall Cluster uses for communications with the Management Server if the primary control IP address fails.

   c) If the Firewall Cluster's primary control IP address and backup control IP address are dynamic or if the Firewall Cluster is in an environment where only the Firewall Cluster can initiate connections to the Management Server, select **Node-initiated contact to Management Server**.

   When this option is selected, the Firewall Cluster opens a connection to the Management Server and maintains connectivity.

   d) From the **Primary** heartbeat drop-down list, select the primary interface for communications between the nodes.

   We recommend using a physical interface, not a VLAN interface. We strongly recommend that you do not direct any other traffic through this interface. A dedicated network (without other traffic) is recommended for security and reliability of heartbeat communication.

   CAUTION

   Primary and backup heartbeat networks exchange confidential information. If dedicated networks are not possible, configure the cluster to encrypt the exchanged information.

   e) From the **Backup** heartbeat drop-down list, select the backup heartbeat interface that is used if the primary heartbeat interface is unavailable.

   It is not mandatory to configure a backup heartbeat interface, but we strongly recommend it. If heartbeat traffic is not delivered, the cluster cannot operate and traffic is disturbed. We strongly recommend that you use a dedicated interface for the backup heartbeat as well.

f) From the **Identity for Authentication Requests** drop-down list, select the IP address that identifies the firewall to external authentication servers.

Note

This selection has no effect on routing.

g) (Optional) From the **Source for Authentication Requests** drop-down list, select the IP address that identifies the firewall when it sends an authentication request to an external authentication server over a VPN.

Note

This selection has no effect on routing.

h) From the **Default IP Address for Outgoing Traffic** field, select the IP address that the nodes use if they have to initiate connections through an interface that has no Node Dedicated IP address.

3) Click **Save**.

Next steps

Continue the configuration in one of the following ways:

- If an interface used for external connections has only a Cluster Virtual IP address, add manual ARP entries for the nodes.
- Bind the engine licenses to the nodes in the Firewall Cluster.

Related tasks

Add manual ARP entries for Firewall Clusters on page 120
Bind engine licenses to Firewall Cluster elements on page 121

Add manual ARP entries for Firewall Clusters

ARP entries are normally managed automatically based on the Firewall's routing configuration. However, you can also add manual ARP entries for the nodes.

If an interface used for external connections has only a cluster virtual IP address (CVI), you must add a static ARP entry. This entry gives the node a permanent reference to an IP address and MAC address.

Steps

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

1) In the navigation pane on the left, select **Interfaces** > **ARP Entries**.

2) Click **Add ARP Entry**.
A new entry is added to the table.

3) Click **Type** and select **Static**.

4) Click **Interface ID** and select the interface on which the ARP entry is applied.

5) Double-click **IP Address** and enter the IP address information.

6) Double-click **MAC Address** and enter the MAC address information.

7) Click **OK**.

8) Click **Save**, then close the Engine Editor.

Next steps

Bind the engine licenses to the nodes of the Firewall Cluster.

Bind engine licenses to Firewall Cluster elements

After you have configured the Firewall Cluster elements, you must manually bind Management Server POL-bound licenses to specific nodes in Firewall Cluster elements.

Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. POS-bound appliance licenses are automatically bound to the correct Firewall element when the engine is fully installed. Each engine is licensed separately even when the engines are clustered.

Steps

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

1) Select **Configuration**, then browse to **Administration**.

2) Browse to **Licenses** > **Engine** or **Licenses** > **Firewall** depending on the type of licenses you have.
All installed licenses appear in the right pane.

3) Right-click a Management Server POL-bound license and select **Bind**.

4) Select the node and click **Select**.
The license is now bound to the selected Firewall element.

Tip

If you bound the license to an incorrect element, right-click the license and select **Unbind**.

CAUTION

When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently bound licenses can't be rebound to another engine without relicensing or deleting the engine element the license is bound to. Until you do that, the unbound license is shown as Retained.

Next steps

Transfer the configuration to the Firewall engines.

Related concepts

Options for initial configuration on page 181

Chapter 6

Configuring Forcepoint NGFW for the IPS role

Contents

Configuring engine elements in the SMC prepares the SMC to manage Forcepoint NGFW in the IPS role.

Types of interfaces for NGFW Engines in the IPS and Layer 2 Firewall roles

Interface definitions are an important part of IPS and Layer 2 Firewall elements.

Types of interfaces for NGFW Engines in the IPS and Layer 2 Firewall roles

Interface type	Purpose of interface	Limitations
Physical (Normal type)	System communications. These interfaces are used when the engine is the source or the final destination of the communications. An example is control communications between the engine and the Management Server. Define at least one interface that is dedicated to system communications for each IPS engine or Layer 2 Firewall.	
Physical (Capture Interface or Inline Interface type)	Traffic inspection. Define one or more traffic inspection interfaces for each IPS engine or Layer 2 Firewall.	

Interface type	Purpose of interface	Limitations
VLAN	Divides a single physical interface into several virtual interfaces.	■ You cannot add VLAN Interfaces on top of other VLAN Interfaces (nested VLANs). ■ You cannot create valid VLAN Interfaces in a Virtual NGFW Engine if the Master NGFW Engine interface that hosts the Virtual NGFW Engine is a VLAN Interface.

Interface numbering

The interfaces have their own numbering in the SMC called the interface ID. The interface IDs are mapped to the corresponding network interfaces on the NGFW Engine when you configure the Forcepoint NGFW software.

Interface numbering for NGFW Engines

Interface type	Interface numbering in the SMC
Layer 3 physical (Firewall/VPN role)	Each physical interface has a unique interface ID number.
Layer 2 physical (Firewall/VPN role)	
Physical (IPS and Layer 2 Firewall roles)	
VLAN	Each VLAN interface has a VLAN number. The defined VLAN interfaces are displayed, for example, as “5.202” for network interface 5 with VLAN 202.
ADSL	Each ADSL interface has a unique interface ID number. ADSL interfaces are only supported on legacy Forcepoint NGFW appliances.
Wireless	The wireless interface has a unique interface ID number. An SSID (service set identifier) interface represents an 802.11 wireless LAN. You can add several SSID interfaces to the wireless interface.
Modem	Modem Interfaces are identified with modem numbers. The modem number is mapped to the modem’s IMEI (international mobile equipment identity) number. Each modem is assigned a unique ID when you connect the modem to the engine. You can change the mapping between the modem’s IMEI number and the modem ID through the engine command line, if necessary.
Tunnel	Tunnel interfaces are numbered with tunnel interface ID numbers. The mapping of Tunnel Interfaces to physical network interfaces on the engine is done automatically by the engine operating system based on the routing configuration.

Interface type	Interface numbering in the SMC
Integrated switch	Integrated switches are identified with switch IDs. Integrated switches have predefined switch IDs. For example, the switch ID is 0 on Forcepoint NGFW 110 appliances. You can add port group interfaces to switches. Port group interfaces are identified by port group IDs. The defined switches and port group interfaces are displayed, for example, as *0.1* for switch ID 0 with port group 1.

Install licenses for NGFW Engines

Install the NGFW Engine licenses that you downloaded while preparing for installation.

Before you begin

The license files must be available to the computer that you use to run the Management Client.

You can install all licenses at the same time even though you have not yet created all elements that the licenses are bound to.

Steps

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

1) In the Management Client, select **Menu** > **System Tools** > **Install Licenses**.

2) Select one or more license files to install in the dialog box that opens and click **Install**.

3) To check that the licenses were installed correctly, select **Configuration**, then browse to **Administration** > **Licenses** > **All Licenses**.
   One license is shown for each NGFW Engine node. You must bind POL-bound licenses manually to the correct NGFW Engine nodes after you have configured the NGFW Engine elements. POS-bound licenses are automatically bound to the NGFW Engine nodes when you install a policy on the NGFW Engine after the NGFW Engine makes initial contact with the Management Server.

Next steps

Define the engine elements.

Configuring IPS engines

IPS elements are a tool for configuring nearly all aspects of your physical IPS components.

Little configuration is done directly on the engines. Most of the configuration is done using the Management Client. You cannot successfully install the engines before defining them in the SMC as outlined.

After you have the SMC installed and running, you can configure the IPS engines.

The tasks you must complete are as follows:

1) Add Single IPS or IPS Cluster elements.

2) Add system communication interfaces.

3) Add traffic inspection interfaces.

4) Bind licenses to specific IPS elements.

Add IPS elements

To add IPS engines to the SMC, add a Single IPS element or an IPS Cluster element that stores the configuration information related to the IPS engine.

This procedure covers the basic configuration of IPS engine elements. For complete instructions about configuring IPS engines, see the *Forcepoint Next Generation Firewall Product Guide*.

Steps

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

1) Select **Configuration**.

2) Right-click **NGFW Engines** and select one of the following:
   - **New** > **IPS** > **IPS Cluster**
   - **New** > **IPS** > **Single IPS**

   The Engine Editor opens.

3) In the **Name** field, enter a unique name.

4) From the **Log Server** drop-down list, select the Log Server for storing this IPS engine's logs.
   If no Log Server is selected, the engine does not make any traffic recordings.

5) (Optional) In the **DNS IP Addresses** list, add one or more DNS IP addresses.
   These addresses are the IP addresses of the DNS servers that the IPS engine uses to resolve domain names and web filtering categorization services (which are defined as URLs).
   - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog that opens.
   - To define an IP address by using a network element, click **Add** and select **Network Element**. Select a Host or External DNS Server element.

6) From the **Location** drop-down list, select the Location to which the IPS belongs.

7) Click **Save**.
   Do not close the Engine Editor.

Add system communication interfaces to IPS engines

Each IPS engine needs at least one interface for communicating with the SMC.

You can add more than one system communication interface to provide a primary and a backup interface for Management Server communications.

Add physical interfaces to IPS elements

Add a physical interface for system communications.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.
2) Right-click the empty space and select **New Physical Interface**.
3) From the **Interface ID** drop-down list, select an ID number.
   This ID maps to a network interface during the initial configuration of the engine.
4) From the **Type** drop-down list, select **Normal Interface**.
5) Click **OK**.
   The physical interface is added to the interface list
6) Click **Save**.
   Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLANs to the physical interface.
- Add IP addresses to the physical interface.

Related tasks

Add static IPv4 addresses to Single IPS interfaces on page 128
Add IP addresses to IPS Cluster interfaces on page 131

Add VLAN interfaces to IPS elements

VLANs divide a single physical network link into several virtual links.

You can add up to 4094 VLANs to each physical interface.

CAUTION

Do not add any manual VLAN definitions to an interface you want to use for sending resets. Adding VLANs prevents selecting the interface as a reset interface and also removes the reset interface from any existing selections.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.
2) Right-click a physical interface and select **New** > **VLAN Interface**.
3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).

Note

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.

4) Click **OK**.
   The specified VLAN ID is added to the physical interface.
5) Click **Save**.
   Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Add static IPv4 addresses to Single IPS interfaces

You can add one or more static IPv4 addresses to each physical or VLAN interface on a Single IPS engine.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.
2) Right-click a Physical Interface or a VLAN Interface and select **New** > **IPv4 Address**.
3) In the **IPv4 Address** field, enter the IPv4 address.

Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

4) Click **Netmask** and adjust the automatically added netmask if necessary.
   The **Network Address** and **Broadcast IP Address** are updated accordingly

5) If the interface is used for system communications and NAT is applied, add contact addresses.
   a) Enter the default contact address in one of the following ways:
      - In the **Default** field, enter the contact address.
      - Select **Dynamic** and define the translated IP address of this component.

   b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.

6) Click **OK**.
   The IP address is added to the interface.

7) Click **Save**.
   If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.

Tip

Write down the networks to which each Interface ID is connected.

Add dynamic IPv4 addresses to Single IPS interfaces

You can add one dynamic IPv4 address to each physical or VLAN interface on a Single IPS engine.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a Physical Interface or a VLAN Interface and select **New** > **IPv4 Address**.

3) Select **Dynamic**.

4) From the **Dynamic Index** drop-down list, select a DHCP index.
   The index is used for identification in other parts of the configuration (such as IPS Policies) to represent the possibly changing IP address.

5) If the interface is used for system communications and NAT is applied, add contact addresses.
   a) Enter the default contact address in one of the following ways:
      - In the **Default** field, enter the contact address.
      - Select **Dynamic** and define the translated IP address of this component.

b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.

6) Click **OK**.
The IP address is added to the interface.

7) Click **Save**.
If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.

Tip

Write down the networks to which each Interface ID is connected.

Add static IPv6 addresses to Single IPS interfaces

You can add one or more static IPv6 addresses to each physical or VLAN interface on a Single IPS engine.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a Physical Interface or a VLAN Interface and select **New** > **IPv6 Address**.

3) In the **IPv6 Address** field, enter the IPv6 address.

Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

4) Click **Prefix Length** and adjust the automatically added prefix length if necessary.

5) Click **OK**.
The IP address is added to the interface.

6) Click **Save**.
If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.

Tip

Write down the networks to which each Interface ID is connected.

Add dynamic IPv6 addresses to Single IPS interfaces

You can add one dynamic IPv6 address to each physical or VLAN interface on a Single IPS engine.

Steps

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

1) In the navigation pane on the left, browse to **Interfaces**.

2) Right-click a Physical Interface or a VLAN Interface and select **New** > **IPv6 Address**.

3) Select **Dynamic**.

4) From the **Dynamic Index** drop-down list, select a DHCP index.
   The index is used for identification in other parts of the configuration (such as IPS Policies) to represent the possibly changing IP address.

5) If the interface is used for system communications and NAT is applied, add contact addresses.
   a) Enter the default contact address in one of the following ways:
      - In the **Default** field, enter the contact address.
      - Select **Dynamic** and define the translated IP address of this component.

   b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.

6) (Optional) If you do not want a default route to be automatically created through the interface, deselect **Automatic Default Route**.

7) (Optional) If you want to use DHCPv6 to get the IPv6 address, select **Use DHCPv6 to get IPv6 Address**.

8) Click **OK**.
   The IP address is added to the interface.

9) Click **Save**.
   If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.

Tip

Write down the networks to which each Interface ID is connected.

Add IP addresses to IPS Cluster interfaces

You can add IP addresses to each node of an IPS Cluster.

You can add both IPv4 and IPv6 addresses to the same interface.

Steps

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

1) In the navigation pane on the left, browse to **Interfaces**.

2) Right-click a physical interface or a VLAN interface and add the IP address in one of the following ways:
   - To add an IPv4 address, select **New** > **IPv4 Address**
   - To add an IPv6 address, select **New** > **IPv6 Address**

3) Click the **IPv4 Address** or **IPv6 Address** cell in the table and enter the IP address for each node.

   Tip

   To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

4) (IPv4 addresses only) If necessary, double-click the **Contact Address** cell in the table and define the contact address for each node.
   - In the **Default** field at the top of the dialog box, enter the default contact address. The default contact address is used by default whenever a component that belongs to another Location connects to this interface.
   - If components from some Locations cannot use the default contact address, click **Add** to define Location-specific contact addresses.

5) (IPv4 addresses only) Check the automatically filled-in **Netmask** and adjust it as necessary.

6) (IPv6 addresses only) Check the automatically filled-in **Prefix Length** and adjust it as necessary.

7) Click **OK**.

8) Click **Save**.

Next steps

Continue the configuration in one of the following ways:

- Select system communication roles for the interfaces.
- Add traffic inspection interfaces.

Select system communication roles for IPS interfaces

Select which interfaces are used for particular roles in system communications.

For example, you can select which IP addresses are used in communications between the IPS engine and the Management Server.

The interfaces you have defined are shown as a tree-table on the Interfaces tab. Global interface options have codes in the tree-table.

Interface option codes

Code	Description
C	The interfaces that have the primary and backup control IP addresses.
(IPS Cluster only) H	The primary and backup heartbeat Interfaces.
O	The default IP address for outgoing connections.

Steps

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

1) In the navigation pane on the left, browse to **Interfaces** > **Interface Options**.

2) Select the interface options.

   a) From the **Primary** control IP address drop-down list, select the primary control IP address that the IPS engine uses for communications with the Management Server.

   b) (Optional, recommended) In the **Backup** control IP address drop-down list, select a backup control IP address that the IPS engine uses for communications with the Management Server if the primary control IP address fails.

   c) (IPS Cluster only) From the **Primary** heartbeat drop-down list, select the primary interface for communications between the nodes.

   We recommend using a physical interface, not a VLAN interface. We strongly recommend that you do not direct any other traffic through this interface. A dedicated network (without other traffic) is recommended for security and reliability of heartbeat communication.

   CAUTION

   Primary and backup heartbeat networks exchange confidential information. If dedicated networks are not possible, configure the cluster to encrypt the exchanged information.

   d) (IPS Cluster only) From the **Backup** heartbeat drop-down list, select the backup heartbeat interface that is used if the primary heartbeat interface is unavailable.

   It is not mandatory to configure a backup heartbeat interface, but we strongly recommend it. If heartbeat traffic is not delivered, the cluster cannot operate and traffic is disturbed. We strongly recommend that you use a dedicated interface for the backup heartbeat as well.

   e) (Single IPS only) If the Single IPS engine's primary control IP address and backup control IP address are dynamic or if the Single IPS engine is in an environment where only the IPS engine can initiate connections to the Management Server, select **Node-initiated contact to Management Server**.

   When this option is selected, the engine opens a connection to the Management Server and maintains connectivity.

   f) From the **Default IP Address for Outgoing Traffic** drop-down list, select the IP address that nodes use if they have to initiate connections through an interface that has no Node Dedicated IP address.

3) Click **Save**.

Next steps

Add traffic inspection interfaces for the IPS engine.

Add traffic inspection interfaces to IPS engines

IPS engines pick up passing network traffic for inspection in real time.

You can define both capture interfaces and inline interfaces for the same IPS engine.

When traffic is inspected, it might be important to know the interface through which it arrives to the IPS engine. It is also important to be able to distinguish an IPS engine's capture interfaces from its inline interfaces. Logical interface elements are used for both these purposes. They allow you to group interfaces that belong to the same network segment and to identify the type of the traffic inspection interface.

Define a logical interface in the following cases:

- You want to create both capture interfaces and inline interfaces on the same IPS engine.
- You want to distinguish interfaces from each other.

Next steps

Continue the configuration in one of the following ways:

- If you want to use reset interfaces with capture interfaces, add reset interfaces.
- Add capture interfaces or inline interfaces.

Add logical interfaces to IPS engines

Logical Interface elements are used in the IPS Policy and the traffic inspection process to represent a network segment.

The SMC contains one default Logical Interface element. A logical interface can represent any number or combination of physical interfaces and VLAN interfaces. However, the same logical interface cannot be used to represent both capture interfaces and inline interfaces on the same IPS engine. The rules in the ready-made IPS Template policy match all logical interfaces.

Steps

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

1) Select **Configuration**.

2) Expand the **Other Elements** branch.

3) Right-click **Logical Interfaces** and select **New Logical Interface**.

4) In the **Name** field, enter a unique name.

5) (Optional) If you use VLAN tagging, select **View interface as one LAN**.
   By default, the IPS engine treats a single connection as multiple connections when an external switch passes traffic between different VLANs and all traffic is mirrored to the IPS engine through a SPAN port.

6) Click **OK**.

Next steps

Continue the configuration in one of the following ways:

- If you want to use reset interfaces with capture interfaces, add reset interfaces.
- Add capture interfaces or inline interfaces.

Related tasks

Add capture interfaces to IPS engines on page 136
Add inline interfaces to IPS engines on page 137

Add reset interfaces to IPS engines

Reset interfaces can deliver TCP resets and ICMP destination unreachable messages to interrupt communications picked up from capture interfaces when the communications trigger a response.

VLANs are supported for sending resets, but the correct VLAN is selected automatically. An interface you want to use as the reset interface must not have any manually added VLAN configuration.

The reset interface must be in the same broadcast domain as the capture interface that uses the reset interface. The resets are sent using the IP addresses and MAC addresses of the communicating hosts.

Important

An interface that is used only as a reset interface must not have an IP address.

Steps

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

1) Right-click the IPS engine and select **Edit <element type>**.
   The Engine Editor opens.
2) In the navigation pane on the left, browse to **Interfaces**.
3) Right-click the empty space and select **New Physical Interface**.
4) From the **Interface ID** drop-down list, select an ID number.
5) From the **Type** drop-down list, select **Normal Interface**.
6) Click **OK**.
7) Click **Save**.

Result

This interface can now be used as a reset interface. When you set up the physical network, make sure that the reset interface connects to the same network as the capture interfaces.

Add capture interfaces to IPS engines

Capture interfaces monitor traffic that external devices have duplicated for inspection to the IPS engine.

You can have as many capture interfaces as there are available physical ports on the IPS engine (there are no license restrictions regarding this interface type).

External equipment must be set up to mirror traffic to the capture interface. You can connect a capture interface to an external switch SPAN port or a network TAP to capture traffic.

Steps

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

1) Right-click the IPS engine and select **Edit <element type>**.
   The Engine Editor opens.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click the empty space and select **New Physical Interface**.

4) From the **Interface ID** drop-down list, select an ID number.

5) From the **Type** drop-down list, select **Capture Interface**.

6) (Optional) From the **Reset Interface** drop-down list, select a TCP reset interface for traffic picked up through this capture interface.

7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
   - Select an existing Logical Interface element from the list.
   - Click **Select** and browse to another Logical Interface element.
   - Click **New** to create a Logical Interface element, then click **OK**.

8) If you want the IPS engine to inspect traffic from VLANs that are not included in the IPS engine's interface configuration, leave **Inspect Unspecified VLANs** selected.

9) If you want the IPS engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.

10) Click **OK**.

11) Click **Save**.

Next steps

Continue the configuration in one of the following ways:

- Define Inline Interfaces.
- Define how the IPS engine handles traffic when the traffic load is too high using the **Bypass Traffic on Overload** setting.
- Bind engine licenses to IPS elements.

Related tasks

Bypass traffic on overload on page 138
Bind engine licenses to IPS elements on page 139

Add inline interfaces to IPS engines

There are two interfaces in an inline interface. The traffic is forwarded from one interface to the other.

The traffic that the IPS engine allows goes through the inline interface as if it was going through a network cable. The IPS engine drops the traffic you want to stop.

Inline interfaces are associated with a Logical interface element. The Logical interface is used in the IPS policies and the traffic inspection process to represent one or more IPS engine interfaces.

Fail-open network cards have fixed pairs of ports. Make sure to map these ports correctly during the initial configuration of the engine. Otherwise, the network cards do not correctly fail open when the IPS engine is offline. If you use the automatic USB memory stick configuration method for the engine's initial configuration, the ports are configured automatically.

Steps

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

1) Right-click the IPS engine and select **Edit <element type>**.
   The Engine Editor opens.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click the empty space and select **New Physical Interface**.

4) From the **Interface ID** drop-down list, select an ID number.

5) From the **Type** drop-down list, select **Inline Interface**.

6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.

7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
   - Select an existing Logical Interface element from the list.
   - Click **Select** and browse to another Logical Interface element.
   - Click **New** to create a Logical Interface element, then click **OK**.

8) If you want the IPS engine to inspect traffic from VLANs that are not included in the IPS engine's interface configuration, leave **Inspect Unspecified VLANs** selected.

9) If you want the IPS engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.

10) Click **OK**.

11) Click **Save**.

Next steps

Continue the configuration in one of the following ways:

- Define how the IPS engine handles traffic when the traffic load is too high using the **Bypass Traffic on Overload** setting.
- Bind engine licenses to IPS elements.

Related tasks

Bind engine licenses to IPS elements on page 139
Configure Forcepoint NGFW software using automatic configuration on page 187

Bypass traffic on overload

You can configure the IPS engine to bypass traffic when the traffic load becomes too high.

By default, IPS engines inspect all connections. If the traffic load is too high for the IPS engine to inspect all connections, IPS engines can dynamically reduce the number of inspected connections. This reduction can improve performance in evaluation environments, but some traffic might pass through without any access control or inspection.

CAUTION

Using bypass mode requires a fail-open network interface card. If the ports that represent the interfaces cannot fail open, policy installation fails on the engine. Bypass mode is not compatible with VLAN retagging. In network environments where VLAN retagging is used, normal mode is automatically enforced.

Steps

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

1) Right-click the IPS engine and select **Edit <element type>**.
   The Engine Editor opens.
2) In the navigation pane on the left, select **Advanced Settings**.
3) Select **Bypass Traffic on Overload**.
4) Click **Save**.

Next steps

Bind engine licenses to IPS elements.

Bind engine licenses to IPS elements

After you have configured the IPS elements, you must manually bind Management Server POL-bound licenses to specific IPS elements.

Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. POS-bound appliance licenses are automatically bound to the correct IPS element when the engine is fully installed. Each engine is licensed separately even when the engines are clustered.

Steps

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

1) Select **Configuration**, then browse to **Administration**.

2) Browse to **Licenses** > **Engine** or **Licenses** > **IPS** depending on the type of licenses you have.
   All installed licenses appear in the right pane.

3) Right-click a Management Server POL-bound license and select **Bind**.

4) Select the IPS element and click **Select**.
   The license is now bound to the selected IPS element.

Tip

If you bound the license to an incorrect element, right-click the license and select **Unbind**.

CAUTION

When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently bound licenses can't be rebound to another engine without relicensing or deleting the engine element the license is bound to. Until you do that, the unbound license is shown as Retained.

Next steps

Transfer the configuration to the IPS engines.

Chapter 7

Configuring Forcepoint NGFW for the Layer 2 Firewall role

Contents

Configuring engine elements in the SMC prepares the SMC to manage NGFW Engines in the Layer 2 Firewall role.

Types of interfaces for NGFW Engines in the IPS and Layer 2 Firewall roles

Interface definitions are an important part of IPS and Layer 2 Firewall elements.

Types of interfaces for NGFW Engines in the IPS and Layer 2 Firewall roles

Interface type	Purpose of interface	Limitations
Physical (Normal type)	System communications. These interfaces are used when the engine is the source or the final destination of the communications. An example is control communications between the engine and the Management Server. Define at least one interface that is dedicated to system communications for each IPS engine or Layer 2 Firewall.	
Physical (Capture Interface or Inline Interface type)	Traffic inspection. Define one or more traffic inspection interfaces for each IPS engine or Layer 2 Firewall.	

Interface type	Purpose of interface	Limitations
VLAN	Divides a single physical interface into several virtual interfaces.	■ You cannot add VLAN Interfaces on top of other VLAN Interfaces (nested VLANs). ■ You cannot create valid VLAN Interfaces in a Virtual NGFW Engine if the Master NGFW Engine interface that hosts the Virtual NGFW Engine is a VLAN Interface.

Install licenses for NGFW Engines

Install the NGFW Engine licenses that you downloaded while preparing for installation.

Before you begin

The license files must be available to the computer that you use to run the Management Client.

You can install all licenses at the same time even though you have not yet created all elements that the licenses are bound to.

Steps

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

1) In the Management Client, select **Menu** > **System Tools** > **Install Licenses**.

2) Select one or more license files to install in the dialog box that opens and click **Install**.

3) To check that the licenses were installed correctly, select **Configuration**, then browse to **Administration** > **Licenses** > **All Licenses**.

   One license is shown for each NGFW Engine node. You must bind POL-bound licenses manually to the correct NGFW Engine nodes after you have configured the NGFW Engine elements. POS-bound licenses are automatically bound to the NGFW Engine nodes when you install a policy on the NGFW Engine after the NGFW Engine makes initial contact with the Management Server.

Next steps

Define the engine elements.

Configuring Layer 2 Firewalls

Layer 2 Firewall elements are a tool for configuring nearly all aspects of your Layer 2 Firewalls.

Little configuration is done directly on the engines. Most of the configuration is done using the Management Client. The engines cannot be successfully installed before defining them in the SMC as outlined.

After you have the SMC installed and running, you can configure the Layer 2 Firewalls.

The tasks you must complete are as follows:

1) Add Single Layer 2 Firewall or Layer 2 Firewall Cluster elements.

2) Add system communication interfaces.

3) Add traffic inspection interfaces.

4) Bind licenses to specific Layer 2 Firewall elements.

Add Layer 2 Firewall elements

The basic configuration of Layer 2 Firewall engine elements begins with creating an engine element.

Steps

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

1) In the Management Client, select **Configuration**.

2) Right-click **NGFW Engines** and select one of the following:
   - **New** > **Layer 2 Firewall** > **Layer 2 Firewall Cluster**
   - **New** > **Layer 2 Firewall** > **Single Layer 2 Firewall**

   The Engine Editor opens.

3) In the **Name** field, enter a unique name.

4) From the **Log Server** drop-down list, select the Log Server that stores the log events that the Layer 2 Firewall engine creates.

5) (Optional) In the **DNS IP Addresses** field, add one or more DNS IP addresses for the Layer 2 Firewall engine.

   These addresses are the IP addresses of the DNS servers that the Layer 2 Firewall engine uses to resolve domain names and web filtering categorization services (which are defined as URLs).
   - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog box that opens.
   - To define an IP address by using a Network element, click **Add** and select **Network Element**. Select a predefined Alias element that represents the IP address of the DNS of a dynamic network interface, a Host element, or an External DNS Server element.

6) From the **Location** drop-down list, select the location for this engine if there is a NAT device between SMC components affecting this engine's communications.

7) Click **Save**.

   Do not close the Engine Editor.

Add system communications interfaces to Layer 2 Firewalls

Each Layer 2 Firewall needs at least one interface for communicating with the SMC.

You can add more than one system communication interface to provide a primary and a backup interface for Management Server communications.

Add physical interfaces to Layer 2 Firewalls

Add a physical interface for system communications.

Steps

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

1) In the navigation pane on the left, browse to **Interfaces**.
2) Right-click the empty space and select **New Physical Interface**.
3) From the **Interface ID** drop-down list, select an ID number.
   This ID maps to a network interface during the initial configuration of the engine.
4) From the **Type** drop-down list, select **Normal Interface**.
5) Click **OK**.
   The physical interface is added to the interface list.
6) Click **Save**.
   Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLANs to the physical interface.
- Add an IP address to the physical interface.

Related tasks

Add static IPv4 addresses to Single Layer 2 Firewall interfaces on page 145
Add IP addresses to Layer 2 Firewall Cluster interfaces on page 149

Add VLAN Interfaces to Layer 2 Firewalls

VLANs divide a single physical network link into several virtual links.

You can add up to 4094 VLANs to each physical interface.

CAUTION

Do not add any manual VLAN definitions to an interface you want to use for sending resets. Adding VLANs prevents selecting the interface as a reset interface and also removes the reset interface from any existing selections.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.
2) Right-click a physical interface and select **New** > **VLAN Interface**.
3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).

Note

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.

4) Click **OK**.
   The specified VLAN ID is added to the physical interface.
5) Click **Save**.
   Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Add static IPv4 addresses to Single Layer 2 Firewall interfaces

You can add one or more static IPv4 addresses to each physical or VLAN interface on a Single Layer 2 Firewall.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.
2) Right-click a Physical Interface or a VLAN Interface and select **New** > **IPv4 Address**.
3) In the **IPv4 Address** field, enter the IPv4 address.

Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

4) Click **Netmask** and adjust the automatically added netmask if necessary.
   The **Network Address** and **Broadcast IP Address** are updated accordingly

5) If the interface is used for system communications and NAT is applied, add contact addresses.
   a) Enter the default contact address in one of the following ways:
      - In the **Default** field, enter the contact address.
      - Select **Dynamic** and define the translated IP address of this component.

   b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.

6) Click **OK**.
   The IP address is added to the interface.

7) Click **Save**.
   If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.

Tip

Write down the networks to which each Interface ID is connected.

Add dynamic IPv4 addresses to Single Layer 2 Firewall interfaces

You can add one dynamic IPv4 address to each physical or VLAN interface on a Single Layer 2 Firewall.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a Physical Interface or a VLAN Interface and select **New** > **IPv4 Address**.

3) Select **Dynamic**.

4) From the **Dynamic Index** drop-down list, select a DHCP index.
   The index is used for identification in other parts of the configuration (such as IPS Policies) to represent the possibly changing IP address.

5) If the interface is used for system communications and NAT is applied, add contact addresses.
   a) Enter the default contact address in one of the following ways:
      - In the **Default** field, enter the contact address.
      - Select **Dynamic** and define the translated IP address of this component.

b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.

6) Click **OK**.
The physical interface is added to the interface list.

7) Click **Save**.
If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.

Tip

Write down the networks to which each Interface ID is connected.

Add static IPv6 addresses to Single Layer 2 Firewall interfaces

You can add one or more static IPv6 addresses to each physical or VLAN interface on a Single Layer 2 Firewall.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a Physical Interface or a VLAN Interface and select **New** > **IPv6 Address**.

3) In the **IPv6 Address** field, enter the IPv6 address.

Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

4) Click **Prefix Length** and adjust the automatically added prefix length if necessary.

5) Click **OK**.
The IP address is added to the interface.

6) Click **Save**.
If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.

Tip

Write down the networks to which each Interface ID is connected.

Add dynamic IPv6 addresses to Single Layer 2 Firewall interfaces

You can add one dynamic IPv6 address to each physical or VLAN interface on a Single Layer 2 Firewall.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a physical interface or a VLAN interface and select **New** > **IPv6 Address**.

3) Select **Dynamic**.

4) From the **Dynamic Index** drop-down list, select a DHCP index.
   The index is used for identification in other parts of the configuration (such as IPS Policies) to represent the possibly changing IP address.

5) If the interface is used for system communications and NAT is applied, add contact addresses.
   a) Enter the default contact address in one of the following ways:
      - In the **Default** field, enter the contact address.
      - Select **Dynamic** and define the translated IP address of this component.

   b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.

6) (Optional) If you do not want a default route to be automatically created through the interface, deselect **Automatic Default Route**.

7) (Optional) If you want to use DHCPv6 to get the IPv6 address, select **Use DHCPv6 to get IPv6 Address**.

8) Click **OK**.
   The IP address is added to the interface.

9) Click **Save**.
   If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.

Tip

Write down the networks to which each Interface ID is connected.

Add IP addresses to Layer 2 Firewall Cluster interfaces

Add IP addresses to Layer 2 Firewall Cluster interfaces.

You can add both IPv4 and IPv6 addresses to the same interface.

Steps

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

1) In the navigation pane on the left, select **Interfaces**.

2) Right-click a physical interface or a VLAN interface and add the IP address in one of the following ways:
   - To add an IPv4 address, select **New** > **IPv4 Address**
   - To add an IPv6 address, select **New** > **IPv6 Address**

3) Click the **IPv4 Address** or **IPv6 Address** cell in the table and enter the IP address for each node.

Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

4) (IPv4 addresses only) If necessary, double-click the **Contact Address** cell in the table and define the contact address for each node.
   - In the **Default** field at the top of the dialog box, enter the default contact address. The default contact address is used by default whenever a component that belongs to another Location connects to this interface.
   - If components from some Locations cannot use the default contact address, click **Add** to define Location-specific contact addresses.

5) (IPv4 addresses only) Check the automatically filled-in **Netmask** and adjust it as necessary.

6) (IPv6 addresses only) Check the automatically filled-in **Prefix Length** and adjust it as necessary.

7) Click **OK**.

8) Click **Save**.
   Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Select system communication roles for the interfaces.
- Add traffic inspection interfaces.

Select system communication roles for Layer 2 Firewall interfaces

Select which interfaces are used for particular roles in system communications.

For example, you can select which IP addresses are used in communications between the Layer 2 Firewall and the Management Server.

The interfaces you have defined are shown as a tree-table on the Interfaces tab. Global interface options have codes in the tree-table.

Interface option codes

Code	Description
C	The interfaces that have the primary and backup control IP addresses.
(Layer 2 Firewall Cluster only) H	The primary and backup heartbeat Interfaces.
O	The default IP address for outgoing connections.

Steps

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

1) In the navigation pane on the left, browse to **Interfaces** > **Interface Options**.

2) Select the interface options.

   a) From the **Primary** control IP address drop-down list, select the primary control IP address that the Layer 2 Firewall uses for communications with the Management Server.

   b) (Optional, recommended) In the **Backup** control IP address drop-down list, select a backup control IP address that the Layer 2 Firewall uses for communications with the Management Server if the primary control IP address fails.

   c) (Layer 2 Firewall Cluster only) From the **Primary** heartbeat drop-down list, select the primary interface for communications between the nodes.

   We recommend using a physical interface, not a VLAN interface. We strongly recommend that you do not direct any other traffic through this interface. A dedicated network (without other traffic) is recommended for security and reliability of heartbeat communication.

   CAUTION

   Primary and backup heartbeat networks exchange confidential information. If dedicated networks are not possible, configure the cluster to encrypt the exchanged information.

   d) (Layer 2 Firewall Cluster only) From the **Backup** heartbeat drop-down list, select the backup heartbeat interface that is used if the primary heartbeat interface is unavailable.

   It is not mandatory to configure a backup heartbeat interface, but we strongly recommend it. If heartbeat traffic is not delivered, the cluster cannot operate and traffic is disturbed. We strongly recommend that you use a dedicated interface for the backup heartbeat as well.

e) (Single Layer 2 Firewall only) If the Single Layer 2 Firewall's primary control IP address and backup control IP address are dynamic or if the Single Layer 2 Firewall is in an environment where only the Layer 2 Firewall can initiate connections to the Management Server, select **Node-initiated contact to Management Server**.

When this option is selected, the engine opens a connection to the Management Server and maintains connectivity.

f) From the **Default IP Address for Outgoing Traffic** drop-down list, select the IP address that nodes use if they have to initiate connections through an interface that has no Node Dedicated IP address.

3) Click **Save**.

Next steps

Add traffic inspection interfaces for the Layer 2 Firewall.

Add traffic inspection interfaces to Layer 2 Firewalls

Layer 2 Firewalls pick up passing network traffic for inspection in real time.

You can define both capture interfaces and inline interfaces for the same Layer 2 Firewall.

When traffic is inspected, it might be important to know the interface through which it arrives to the Layer 2 Firewall. It is also important to be able to distinguish a Layer 2 Firewall's capture interfaces from its inline interfaces. Logical Interface elements are used for both these purposes. They allow you to group interfaces that belong to the same network segment and to identify the type of the traffic inspection interface.

Define a logical interface in the following cases:

- You want to create both capture interfaces and inline interfaces on the same Layer 2 Firewall.
- You want to create Logical Interfaces to distinguish interfaces from each other.

Add logical interfaces to Layer 2 Firewalls

A logical interface is used in the Layer 2 Firewall Policy and the traffic inspection process to represent a network segment.

The SMC contains one default Logical Interface element. A logical interface can represent any number or combination of physical interfaces and VLAN interfaces. However, the same logical interface cannot be used to represent both capture interfaces and inline interfaces on the same Layer 2 Firewall. The rules in the ready-made Layer 2 Firewall Template match all logical interfaces.

Steps

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

1) Select **Configuration**.

2) Expand the **Other Elements** branch.

3) Right-click **Logical Interfaces** and select **New Logical Interface**.

4) In the **Name** field, enter a unique name.

5) (Optional) If you use VLAN tagging, select **View interface as one LAN**.
By default, the engine treats a single connection as multiple connections when a switch passes traffic between different VLANs and all traffic is mirrored to the IPS engine through a SPAN port.

6) Click **OK**.

Next steps

Continue the configuration in one of the following ways:

- If you want to use reset interfaces with capture interfaces, add reset interfaces.
- Add capture interfaces or inline interfaces.

Related tasks
Add capture interfaces to Layer 2 Firewalls on page 153
Add inline interfaces to Layer 2 Firewalls on page 154

Add reset interfaces to Layer 2 Firewalls

Reset interfaces can deliver TCP resets and ICMP destination unreachable messages to interrupt communications picked up from capture interfaces when the communications trigger a response.

VLANs are supported for sending resets, but the correct VLAN is selected automatically. An interface you want to use as the reset interface must not have any manually added VLAN configuration.

The reset interface must be in the same broadcast domain as the capture interface that uses the reset interface. The resets are sent using the IP addresses and MAC addresses of the communicating hosts.

Important

An interface that is used only as a reset interface must not have an IP address.

Steps

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

1) Right-click the Layer 2 Firewall element and select **Edit <element type>**.
The Engine Editor opens.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click the empty space and select **New Physical Interface**.

4) From the **Interface ID** drop-down list, select an ID number.

5) From the **Type** drop-down list, select **Normal Interface**.

6) Click **OK**.

7) Click **Save**.
Do not close the Engine Editor.

Result

This interface can now be used as a reset interface. When you set up the physical network, make sure that the reset interface connects to the same network as the capture interfaces.

Next steps

Add capture interfaces and inline interfaces.

Add capture interfaces to Layer 2 Firewalls

Capture interfaces monitor traffic that external devices have duplicated for inspection to the Layer 2 Firewall.

You can have as many capture interfaces as there are available network ports on the Layer 2 Firewall (there are no license restrictions regarding this interface type).

External equipment must be set up to mirror traffic to the capture interface. You can connect a capture interface to an external switch SPAN port or a network TAP to capture traffic.

Steps

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

1) On the **Interfaces** pane, right-click and select **New Physical Interface**.

2) From the **Interface ID** drop-down list, select an ID number.

3) From the **Type** drop-down list, select **Capture Interface**.

4) (Optional) From the **Reset Interface** drop-down list, select a TCP reset interface for traffic picked up through this capture interface.

5) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
   - Select an existing Logical Interface element from the list.
   - Click **Select** and browse to another Logical Interface element.
   - Click **New** to create a Logical Interface element, then click **OK**.

6) If you want the Layer 2 Firewall engine to inspect traffic from VLANs that are not included in the IPS engine's interface configuration, leave **Inspect Unspecified VLANs** selected.

7) If you want the Layer 2 Firewall engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.

8) Click **OK**.

9) Click **Save**.
If you plan to add inline interfaces, do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add inline interfaces.
- Bind engine licenses to Layer 2 Firewall elements.

Related tasks
Bind engine licenses to Layer 2 Firewall elements on page 155

Add inline interfaces to Layer 2 Firewalls

There are two interfaces in an inline interface. The traffic is forwarded from one interface to the other.

The traffic that the Layer 2 Firewall allows goes through the inline interface as if it was going through a network cable. The Layer 2 Firewall drops the traffic you want to stop.

Inline interfaces are associated with a Logical Interface element. The Logical Interface is used in the Layer 2 Firewall Policy and the traffic inspection process to represent one or more Layer 2 Firewall interfaces.

Steps

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

1) Right-click the Layer 2 Firewall and select **Edit <element type>**.
The Engine Editor opens.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click the empty space and select **New Physical Interface**.

4) From the **Interface ID** drop-down list, select an ID number.

5) From the **Type** drop-down list, select **Inline Interface**.

6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.

7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
   - Select an existing Logical Interface element from the list.
   - Click **Select** and browse to another Logical Interface element.
   - Click **New** to create a Logical Interface element, then click **OK**.

8) If you want the Layer 2 Firewall engine to inspect traffic also from VLANs that are not included in the engine's interface configuration, leave **Inspect Unspecified VLANs** selected.

9) If you want the Layer 2 Firewall engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.

10) Click **OK**.

11) Click **Save**, then close the Engine Editor.

Next steps

Bind engine licenses to Layer 2 Firewall elements.

Related tasks
Bind engine licenses to Layer 2 Firewall elements on page 155

Bind engine licenses to Layer 2 Firewall elements

After you have configured the Layer 2 Firewall elements, you must manually bind Management Server POL-bound licenses to specific Layer 2 Firewall elements.

Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. POS-bound appliance licenses are automatically bound to the correct Layer 2 Firewall element when the engine is fully installed. Each engine is licensed separately even when the engines are clustered.

Steps

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

1) Select **Configuration**, then browse to **Administration**.

2) Browse to **Licenses** > **Engine**.
All installed licenses appear in the right pane.

3) Right-click a Management Server POL-bound license and select **Bind**.

4) Select the Layer 2 Firewall element and click **Select**.
The license is now bound to the selected Layer 2 Firewall element.

CAUTION

When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently bound licenses can't be rebound to another engine without relicensing or deleting the engine element the license is bound to. Until you do that, the unbound license is shown as Retained.

Next steps

Transfer the configuration to the Layer 2 Firewall engines.

Chapter 8

Configuring NGFW Engines as Master NGFW Engines and Virtual NGFW Engines

Contents

Configuring engine elements in the SMC prepares the SMC to manage Master NGFW Engines and Virtual NGFW Engines.

Master NGFW Engine and Virtual NGFW Engine configuration overview

Virtual NGFW Engines are logically separate virtual engine instances on a physical engine device. A Master NGFW Engine is a physical engine device that provides resources for Virtual NGFW Engines. One physical Master NGFW Engine can support multiple Virtual NGFW Engines.

Little configuration is done directly on the Master NGFW Engine. No installation or configuration is done on the Virtual NGFW Engines. Most of the configuration is done using the Management Client. The engines cannot be successfully installed before defining them in the Management Client as outlined in this section.

The tasks you must complete are as follows:

1) Add Master NGFW Engine elements.
   a) Add Virtual Resource elements.
   b) Add physical interfaces and optionally VLAN interfaces to the Master NGFW Engine.
   c) Assign Virtual Resources to the interfaces that are used by the Virtual NGFW Engines hosted on the Master NGFW Engine.
2) Add Virtual Firewall, Virtual IPS, or Virtual Layer 2 Firewall elements.
   a) Configure the automatically created physical interfaces.

b) (Optional) Add VLAN interfaces for the Virtual NGFW Engines.

3) Bind licenses to specific nodes of the Master NGFW Engine.

Install licenses for NGFW Engines

Install the NGFW Engine licenses that you downloaded while preparing for installation.

Before you begin

The license files must be available to the computer that you use to run the Management Client.

You can install all licenses at the same time even though you have not yet created all elements that the licenses are bound to.

Steps

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

1) In the Management Client, select **Menu** > **System Tools** > **Install Licenses**.

2) Select one or more license files to install in the dialog box that opens and click **Install**.

3) To check that the licenses were installed correctly, select **Configuration**, then browse to **Administration** > **Licenses** > **All Licenses**.

   One license is shown for each NGFW Engine node. You must bind POL-bound licenses manually to the correct NGFW Engine nodes after you have configured the NGFW Engine elements. POS-bound licenses are automatically bound to the NGFW Engine nodes when you install a policy on the NGFW Engine after the NGFW Engine makes initial contact with the Management Server.

Next steps

Define the engine elements.

Add Master NGFW Engine elements

To introduce a new Master NGFW Engine to the SMC, add a Master NGFW Engine element that stores the configuration information for the Master NGFW Engine and Virtual NGFW Engines.

Steps

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

1) In the Management Client, select **Configuration**.

2) Right-click **NGFW Engines** and select **New** > **Master NGFW Engine**.

3) Select the role for the Virtual NGFW Engines the Master NGFW Engine hosts, then click **OK**.
The Engine Editor opens.

4) In the **Name** field, enter a unique name.

5) Select the **Log Server** to which the Master NGFW Engine sends its log data.

6) (Optional) Define one or more **DNS IP Addresses**.
These addresses are the IP addresses of the DNS servers that the Master NGFW Engine uses to resolve domain names. There are two ways to define IP addresses.
   - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog box that opens.
   - To define an IP address using a network element, click **Add** and select **Network Element**.

7) Select the **Location** for this Master NGFW Engine if there is a NAT device between this Master NGFW Engine and other SMC components.

8) (Optional) If you do not need to use clustering on the Master NGFW Engine:
   a) In the navigation pane on the left, browse to **General** > **ARP Entries**.
   b) Select one of the nodes, then click **Remove Node**.
   c) When prompted to confirm that you want to delete the selected node, click **Yes**.

9) Click **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add more nodes to the Master NGFW Engine.
- Add Virtual Resource elements.

Add nodes to Master NGFW Engines

Add all nodes you plan to install before you begin configuring the interfaces.

The Master NGFW Engine has placeholders for two nodes when the element is created. A Master NGFW Engine can have up to 16 nodes.

Steps

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

1) Right-click the Master NGFW Engine element and select **Edit Master NGFW Engine**.
   The Engine Editor opens.
2) In the navigation pane on the left, select **General** > **Clustering**.
3) Click **Add Node**.
4) (Optional) Change the **Name**.
5) Click **OK**.
   The node is added to the Master NGFW Engine.
6) Click **Save**.

Create Virtual Resource elements

Virtual Resources associate Virtual NGFW Engines with Physical Interfaces or VLAN Interfaces on the Master NGFW Engine.

When you select the same Virtual Resource for a Physical Interface or VLAN Interface on the Master NGFW Engine and for a Virtual NGFW Engine, the Virtual NGFW Engine is automatically associated with the Master NGFW Engine. Create one Virtual Resource for each Virtual NGFW Engine that you plan to add.

Steps

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

1) Select **Configuration**.
2) Right-click the Master NGFW Engine element, then select **Edit Master NGFW Engine**.
3) Browse to **Interfaces** > **Virtual Resources**.
4) Click **Add**.
5) Configure the settings.
6) Click **OK**.
7) Click **Save**.

Next steps

Continue the configuration in one of the following ways:

- Configure Master NGFW Engine interfaces.

- Associate the Virtual Resource with a Master NGFW Engine interface and with a Virtual NGFW Engine.

Types of interfaces for Master NGFW Engines in the Firewall/VPN role

You can configure several types of interfaces for Master NGFW Engines in the Firewall/VPN role.

Types of interfaces for Master NGFW Engines in the Firewall/VPN role

Interface type	Purpose of interface	Limitations
Layer 3 physical	System communications and traffic inspection.	You cannot add both VLAN Interfaces and IP addresses to a Physical Interface. If an IP address is already configured for a Physical Interface, adding a VLAN Interface removes the IP address. If you plan to use VLAN Interfaces, configure the VLAN Interfaces first and then add IP addresses to the VLAN Interfaces.
Layer 2 physical	Traffic inspection. Layer 2 interfaces on Master NGFW Engines in the Firewall/VPN role allow the engine to provide the same kind of traffic inspection that is available for Master NGFW Engines in the IPS and Layer 2 Firewall roles.	■ You cannot add IP addresses to layer 2 physical interfaces on Master NGFW Engines in the Firewall/VPN role. ■ VLAN retagging is not supported on layer 2 physical interfaces of the inline IPS type.
VLAN	Divides a single physical interface into several virtual interfaces.	■ You cannot add VLAN interfaces on top of other VLAN Interfaces (nested VLANs).

Add layer 3 physical interfaces to Master NGFW Engines

Master NGFW Engines can have two types of physical interfaces: interfaces for the Master NGFW Engine's own communications, and interfaces that are used by the Virtual NGFW Engines hosted on the Master NGFW Engine.

You must add at least one physical interface for the Master NGFW Engine's own communications.

For Master NGFW Engine clusters, it is recommended to add at least two physical interfaces:

- An interface used for communications between the Management Server and the Master NGFW Engine.
- An interface for the heartbeat communications between the cluster nodes. The heartbeat traffic is critical to the functioning of the cluster, so it is highly recommended to have a dedicated heartbeat interface.

Steps

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

1) Right-click the Master NGFW Engine element, then select **Edit <element type>**.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Click **Add**, then select **Layer 3 Physical Interface**.

4) (Interface for Master NGFW Engine communications only) Define the physical interface properties.
   a) From the **Type** drop-down list, select the interface type according to the engine role.
   b) Do not select a Virtual Resource for an interface that is used for the Master NGFW Engine's own communications.
   c) In the **Cluster MAC Address** field, enter the MAC address for the Master NGFW Engine.

Note

Do not use the MAC address of any actual network card on any of the Master NGFW Engine nodes.

Note

Make sure that you set the interface speed correctly. When the bandwidth is set, the Master NGFW Engine always scales the total amount of traffic on this interface to the bandwidth you defined. The bandwidth is scaled even if there are no bandwidth limits or guarantees defined for any traffic.

5) (Interface for hosted Virtual NGFW Engine communications only) Define the physical interface properties.
   a) From the **Type** drop-down list, select the interface type according to the engine role.
   b) (Virtual IPS only) From the **Failure Mode** drop-down list, select how traffic to the inline interface is handled if the Virtual IPS engine goes offline.

Note

If there are VLAN interfaces under the inline interface, select **Bypass**.

CAUTION

Using Bypass mode requires the Master NGFW Engine appliance to have a fail-open network interface card. If the ports that represent the pair of inline interfaces on the appliance cannot fail open, the policy installation fails on the Virtual IPS engine. Bypass mode is not compatible with VLAN retagging. In network environments where VLAN retagging is used, normal mode is automatically enforced.

c) From the **Virtual Resource** drop-down list, select the Virtual Resource element associated with the interface.

Select the same Virtual Resource in the properties of the Virtual NGFW Engine to add the **Virtual IPS engine** to the Master NGFW Engine.

Note

Only one Virtual Resource can be selected for each physical interface. If you want to add multiple Virtual Resources, add VLAN interfaces to the physical interface and select the Virtual Resource in the VLAN interface properties.

6) Click **OK**.

The physical interface is added to the interface list.

7) Click **Save**.

Next steps

Continue the configuration in one of the following ways:

- Add VLANs to physical interfaces.
- Add IP addresses to the physical interfaces used for Master NGFW Engine communications.

Add VLAN interfaces to layer 3 interfaces of Master NGFW Engines

Master NGFW Engines can have two types of VLAN interfaces: VLAN interfaces for the Master NGFW Engine's own traffic, and VLAN interfaces that are used by the Virtual NGFW Engines hosted on the Master NGFW Engine.

The maximum number of VLANs for a single physical interface is 4094. The VLANs must also be defined in the configuration of the external switch or router to which the interface is connected.

On Master NGFW Engines that host Virtual IPS engines or Virtual Layer 2 Firewalls, the Virtual NGFW Engines can inspect traffic from VLAN interfaces without configuring VLAN tagging.

Steps

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

1) Right-click a Master NGFW Engine, then select **Edit <element type>**.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click a physical interface, then select **New** > **VLAN Interface**.

4) To associate the VLAN interface with a Virtual NGFW Engine, select a Virtual Resource from the **Virtual Resource** drop-down list.

5) Define the VLAN interface properties.

CAUTION

The throughput for each VLAN interface must not be higher than the throughput for the physical interface to which the VLAN interface belongs.

CAUTION

Make sure that you set the interface speed correctly. When the bandwidth is set, the Master NGFW Engine always scales the total amount of traffic on this interface to the bandwidth you defined. The bandwidth is scaled even if there are no bandwidth limits or guarantees defined for any traffic.

CAUTION

The MTU for each VLAN interface must not be higher than the MTU for the physical interface to which the VLAN interface belongs.

6) Click **OK**.
The specified VLAN ID is added to the physical interface.

7) Click **Save**.
Do not close the Engine Editor.

Next steps

Add IP addresses to the physical interfaces or VLAN interfaces for Master NGFW Engine system communications.

Add IPv4 and IPv6 addresses to Master NGFW Engine interfaces

You can add several IPv4 addresses to each Physical Interface or VLAN Interface that does not have a Virtual Resource associated with it.

Steps

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

1) Right-click a Master NGFW Engine, then select **Edit <element type>**.

2) In the navigation pane on the left, browse to **Interfaces**.

3) Right-click a physical interface or a VLAN interface, then select **New** > **IPv4 Address** or **New** > **IPv6 Address**.

4) Click the **IPv4 Address** or **IPv6 Address** cell in the table, then enter the IP address for each node.

Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

5) (IPv4 addresses only) If necessary, double-click the **Contact Address** cell in the table, then define the contact address for each node.
   - In the **Default** field at the top of the dialog box, enter the default contact address. The default contact address is used by default whenever a component that belongs to another Location connects to this interface.
   - If components from some Locations cannot use the default contact address, click **Add** to define Location-specific contact addresses.

6) (IPv4 addresses only) Check the automatically filled-in **Netmask**, and adjust it as necessary.

7) (IPv6 addresses only) Check the automatically filled-in **Prefix Length**, and adjust it as necessary.

8) Click **OK**.

9) Click **Save**.

Next steps

Continue the configuration in one of the following ways:

- If you are configuring a new Master NGFW Engine, or if you want to change the roles the different interfaces have in the configuration, select system communication roles for Master NGFW Engine interfaces.
- Otherwise, refresh the policy to transfer the configuration changes.

Select system communication roles for Master NGFW Engine interfaces

Select which Master NGFW Engine interfaces are used for particular roles in system communications.

Steps

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

1) Right-click an NGFW Engine, then select **Edit <element type>**.

2) Browse to **Interfaces** > **Interface Options**.

3) In the **Interface Options** pane:

   a) From the **Primary** control IP address drop-down list, select the primary control IP address that the Master NGFW Engine uses for communications with the Management Server.

   Note

   We recommend that you do not use the IP address of an Aggregated Link interface as the primary or secondary control IP address of the NGFW Engine.

   b) (Optional, recommended) From the **Backup** control IP address drop-down list, select a backup control IP address that the Master NGFW Engine uses for communications with the Management Server if the primary control IP address fails.

   c) (Optional, Firewall/VPN role only) If the Master NGFW Engine is behind a device that applies dynamic NAT to outbound connections or in some other way blocks incoming connections, select **Node-Initiated contact to Management Server**.

   When this option is selected, the engine opens a connection to the Management Server and maintains connectivity.

   d) (Master NGFW Engine Cluster Only) From the **Primary** heartbeat drop-down list, select the primary interface for communications between the nodes.

   We recommend using a physical interface, not a VLAN interface. We strongly recommend that you do not direct any other traffic through this interface. A dedicated network helps guarantee reliable and secure operation.

   CAUTION

   Primary and backup heartbeat networks exchange confidential information. If dedicated networks are not possible, configure the cluster to encrypt the exchanged information.

   e) (Master NGFW Engine Cluster Only) From the **Backup** heartbeat drop-down list, select the backup heartbeat interface that is used if the primary heartbeat interface is unavailable.

   It is not mandatory to configure a backup heartbeat interface, but we strongly recommend it. If heartbeat traffic is not delivered, the cluster cannot operate and traffic is disturbed. We strongly recommend that you use a dedicated interface for the backup heartbeat as well.

   f) In the **Default IP Address for Outgoing Traffic** field, select the IP address that the nodes use if they have to initiate connections through an interface that has no Node Dedicated IP address.

4) Click **Save and Refresh**.

Next steps

Bind licenses to Master NGFW Engine elements.

Bind Master NGFW Engine licenses to Master NGFW Engine elements

You must manually bind Management Server POL-bound licenses to a specific Master NGFW Engine element.

Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. POS-bound appliance licenses are automatically bound to the correct Master NGFW Engine element when the engine is fully installed. Virtual NGFW Engines do not require a separate license.

Steps

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

1) Select **Configuration**, then browse to **Administration**.

2) Browse to **Licenses** > **NGFW Engines**.
   All installed licenses appear in the right pane.

3) Right-click a Management Server POL-bound license and select **Bind**.
   The **Select License Binding** dialog box opens.

4) Select the node and click **Select**.
   If you made a mistake, right-click the license and select **Unbind**.

CAUTION

When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently bound licenses cannot be rebound to another engine without relicensing or deleting the engine element the license is bound to. Until you do that, the unbound license is shown as Retained.

Next steps

Add Virtual NGFW Engine elements.

Create Virtual Firewalls

Virtual Firewall elements store the configuration information related to the Virtual Firewalls.

Selecting a Virtual Resource for the Virtual NGFW Engine automatically adds the Virtual NGFW Engine to the Master NGFW Engine where the Virtual Resource is used.

Steps

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

1) Select **Configuration**.

2) Right-click **NGFW Engines** and select **New** > **Firewall** > **Virtual Firewall**.

3) In the **Name** field, enter a unique name.

4) Next to the **Virtual Resource** field, click **Select** and select a Virtual Resource on the Master NGFW Engine to which you want to add the Virtual Firewall.

5) (Optional) In the **DNS IP Addresses** field, add one or more IP addresses.

   DNS IP addresses are IP addresses of external DNS servers. Virtual Firewalls use these DNS servers to resolve Domain names to IP addresses. Virtual Firewalls need DNS resolution to contact services that are defined using URLs or domain names, and to resolve fully qualified domain names (FQDNs) used in policies. When DNS relay is configured, these DNS servers are used unless domain-specific DNS servers are specified in a DNS Relay Profile element.

   Note

   If you have defined NetLink-specific DNS IP addresses, adding DNS IP addresses overrides the NetLink-specific DNS IP addresses.

   - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog box that opens.
   - To define an IP address using a network element, click **Add** and select **Network Element**.

6) (Optional) Next to the **Category** field, click **Select** and select one or more categories.

7) Click **Save**.

   Do not close the Engine Editor.

Next steps

Configure interfaces for the Virtual Firewall.

Configuring physical interfaces for Virtual Firewalls

Physical interfaces for Virtual NGFW Engines represent interfaces allocated to the Virtual NGFW Engine in the Master NGFW Engine.

When you select the Virtual Resource for the Virtual NGFW Engine, physical interfaces are automatically created based on the interface configuration in the Master NGFW Engine properties. The number of physical interfaces depends on the number of interfaces allocated to the Virtual NGFW Engine in the Master NGFW Engine. You cannot create new physical interfaces for Virtual Firewalls. You can optionally change the automatically created physical interfaces. For detailed instructions, see the *Forcepoint Next Generation Firewall Product Guide*.

You can optionally change the automatically created physical interfaces in the Virtual IPS engine properties. For detailed instructions, see the *Forcepoint Next Generation Firewall Product Guide*.

If the configuration of the Master NGFW Engine allows it, you can add VLANs to physical interfaces on the Virtual Firewall. If you do not want to add VLANs, add IP addresses to the physical interfaces.

Add VLAN interfaces to Virtual NGFW Engine interfaces

VLANs divide a single physical network link into several virtual links.

VLAN interfaces can only be added for Virtual NGFW Engines if the creation of VLAN interfaces for Virtual Firewalls is enabled in the Master NGFW Engine Properties. The maximum number of VLANs for a single physical interface is 4094. The VLANs must also be defined in the configuration of the external switch or router to which the interface is connected.

Note

You cannot add VLAN interfaces on top of other VLAN interfaces. Depending on the configuration of the Master NGFW Engine, you might not be able to create valid VLAN interfaces for the Virtual NGFW Engine. Contact the administrator who configured the Master NGFW Engine.

Steps

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

1) Right-click a Virtual Firewall, Virtual IPS engine, or Virtual Layer 2 Firewall and select **Edit <element type>**.
2) In the navigation pane on the left, select **Interfaces**.
3) Right-click a physical interface and select **New** > **VLAN Interface**.
4) Define the VLAN interface properties.

   CAUTION

   The throughput for the Virtual Firewall physical interface must not be higher than the throughput for the Master NGFW Engine interface that hosts the Virtual Firewall. Contact the administrator of the Master NGFW Engine before changing this setting.

   CAUTION

   Make sure that you set the interface speed correctly. When the bandwidth is set, the Virtual NGFW Engine always scales the total amount of traffic on this interface to the bandwidth you defined. The bandwidth is scaled even if there are no bandwidth limits or guarantees defined for any traffic.

5) Click **OK**.
   The specified VLAN ID is added to the physical interface.

Next steps

Continue the configuration in one of the following ways:

- (Virtual Firewall only) If you do not want to add tunnel interfaces for a route-based VPN, add IP addresses directly to the physical interfaces.
- Otherwise, click **Save and Refresh** to transfer the configuration changes.

Add IP addresses for Virtual Firewalls

You can add one or more IPv4 and IPv6 addresses to a Physical Interface or VLAN Interface on a Virtual Firewall.

You can add both IPv4 and IPv6 addresses to the same interface.

Add IPv4 addresses to Virtual Firewall interfaces

You can add one or more static IPv4 addresses for Virtual Firewall interfaces.

Steps

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

1) Right-click a Virtual Firewall and select **Edit Virtual Firewall**.
   The Engine Editor opens.

2) In the navigation pane on the left, select **Interfaces**.
   The **Interfaces** pane opens on the right.

3) Right-click a Physical Interface, VLAN Interface, or Tunnel Interface and select **New** > **IPv4 Address**.

Note

If you have added VLAN Interfaces to Physical Interfaces, add the IPv4 Addresses to the VLAN Interfaces.

4) Enter the **IPv4 Address**.

Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

5) If necessary, define the contact address information.
   - Enter the **Default** contact address. The default contact address is used by default whenever a component that belongs to another Location connects to this interface.
   - If components from some Locations cannot use the Default contact address, click **Exceptions** to define Location-specific contact addresses.

6) Check the automatically filled-in **Netmask** and adjust it as necessary.

7) Click **OK**.

Next steps

Continue the configuration in one of the following ways:

- Add IPv6 addresses.

- If you are creating a new Virtual Firewall, or if you want to change the roles the different interfaces have in the configuration, select interface options for Virtual Firewall interfaces.
- Otherwise, click **Save and Refresh** to transfer the configuration changes.

Add IPv6 addresses to Virtual Firewall interfaces

You can add one or more static IPv6 addresses for Virtual Firewall interfaces.

Steps

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

1) Right-click a Virtual Firewall and select **Edit Virtual Firewall**.
   The Engine Editor opens.

2) In the navigation pane on the left, select **Interfaces**.
   The **Interfaces** pane opens on the right.

3) Right-click a Physical interface and select **New** > **IPv6 Address** or right-click a VLAN Interface and select **New IPv6 Address**.
   The **IP Address Properties** dialog box opens.

   Note

   If you have added VLAN Interfaces to Physical Interfaces, add the IPv6 Addresses to the VLAN Interfaces.

4) Enter the **IPv6 Address**.

   Tip

   To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

5) Check the automatically filled-in **Prefix Length** and adjust it if necessary by entering a value between 0-128.
   The Network Address is automatically generated.

6) Click **OK**.

Next steps

Continue the configuration in one of the following ways:

- If you are creating a new Virtual Firewall, or if you want to change the roles the different interfaces have in the configuration, select interface options for Virtual Firewall interfaces.
- Otherwise, click **Save and Refresh** to transfer the configuration changes.

Select additional options for Virtual Firewall interfaces

In the Virtual Firewall's interface options, you can select which IP addresses are used in particular roles.

Interface Options can only be configured for Virtual Firewalls. All communication between Virtual Firewalls and the SMC is proxied by the Master NGFW Engine. Virtual Firewalls do not have any interfaces for system communication.

Steps

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

1) Right-click an NGFW Engine, then select **Edit <element type>**.
2) Browse to **Interfaces** > **Interface Options**.
3) Configure the settings.

Next steps

Continue the configuration in one of the following ways:

- Add loopback IP addresses for the Virtual Firewall.
- If you are configuring a new Virtual NGFW Engine, click **Save**, close the Engine Editor, then add routes for the Master NGFW Engine.
- Otherwise, click **Save and Refresh** to transfer the configuration changes.

Create Virtual IPS engines

Virtual IPS elements store the configuration information related to the Virtual IPS engines.

Selecting a Virtual Resource for the Virtual NGFW Engine automatically adds the Virtual NGFW Engine to the Master NGFW Engine where the Virtual Resource is used.

Steps

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

1) Select **Configuration**.
2) Right-click **NGFW Engines** and select **New** > **IPS** > **Virtual IPS**.
3) In the **Name** field, enter a unique name.
4) Next to the **Virtual Resource** field, click **Select** and select a Virtual Resource on the Master NGFW Engine to which you want to add the Virtual IPS.

5) (Optional) In the **DNS IP Addresses** field, add one or more IP addresses.

   DNS IP addresses are IP addresses of external DNS servers. Virtual IPS engines use these DNS servers to resolve Domain names to IP addresses. Virtual IPS engines need DNS resolution to contact services that are defined using URLs or domain names, and to resolve fully qualified domain names (FQDNs) used in policies.

   - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog box that opens.
   - To define an IP address using a network element, click **Add** and select **Network Element**.

6) (Optional) Next to the **Category** field, click **Select** and select one or more categories.

7) Click **Save**.

   Do not close the Engine Editor.

Next steps

Configure interfaces for the Virtual IPS engine.

Configuring physical interfaces for Virtual IPS engines

Physical interfaces for Virtual IPS engines represent interfaces allocated to the Virtual IPS engine in the Master NGFW Engine.

When you select the Virtual Resource for the Virtual IPS engine, physical interfaces are automatically created based on the interface configuration of the Master NGFW Engine. The number of physical interfaces depends on the number of interfaces allocated to the Virtual IPS engine in the Master NGFW Engine. It is not recommended to create new physical interfaces in the Virtual IPS engine properties, as they might not be valid.

You can optionally change the automatically created physical interfaces in the Virtual IPS engine properties. For detailed instructions, see the *Forcepoint Next Generation Firewall Product Guide*.

If the configuration of the Master NGFW Engine allows it, you can add VLANs to physical interfaces on the Virtual IPS engine. If you do not want to add VLANs, add IP addresses to the physical interfaces.

Add VLAN interfaces to Virtual NGFW Engine interfaces

VLANs divide a single physical network link into several virtual links.

VLAN interfaces can only be added for Virtual NGFW Engines if the creation of VLAN interfaces for Virtual Firewalls is enabled in the Master NGFW Engine Properties. The maximum number of VLANs for a single physical interface is 4094. The VLANs must also be defined in the configuration of the external switch or router to which the interface is connected.

Note

You cannot add VLAN interfaces on top of other VLAN interfaces. Depending on the configuration of the Master NGFW Engine, you might not be able to create valid VLAN interfaces for the Virtual NGFW Engine. Contact the administrator who configured the Master NGFW Engine.

Steps

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

1) Right-click a Virtual Firewall, Virtual IPS engine, or Virtual Layer 2 Firewall and select **Edit <element type>**.
2) In the navigation pane on the left, select **Interfaces**.
3) Right-click a physical interface and select **New** > **VLAN Interface**.
4) Define the VLAN interface properties.

CAUTION

The throughput for the Virtual Firewall physical interface must not be higher than the throughput for the Master NGFW Engine interface that hosts the Virtual Firewall. Contact the administrator of the Master NGFW Engine before changing this setting.

CAUTION

Make sure that you set the interface speed correctly. When the bandwidth is set, the Virtual NGFW Engine always scales the total amount of traffic on this interface to the bandwidth you defined. The bandwidth is scaled even if there are no bandwidth limits or guarantees defined for any traffic.

5) Click **OK**.
   The specified VLAN ID is added to the physical interface.

Next steps

Continue the configuration in one of the following ways:

- (Virtual Firewall only) If you do not want to add tunnel interfaces for a route-based VPN, add IP addresses directly to the physical interfaces.
- Otherwise, click **Save and Refresh** to transfer the configuration changes.

Add Virtual Layer 2 Firewall elements

Virtual Layer 2 Firewall elements store the configuration information related to the Virtual Layer 2 Firewalls.

Selecting a Virtual Resource for the Virtual Layer 2 Firewall automatically adds the Virtual Layer 2 Firewall to the Master NGFW Engine where the Virtual Resource is used.

Steps

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

1) Select **Configuration**.
2) Right-click **NGFW Engines** and select **New** > **Layer 2 Firewall** > **Virtual Layer 2 Firewall**.
   The Engine Editor opens.

3) In the **Name** field, enter a unique name.

4) Next to the **Virtual Resource** field, click **Select** and select a Virtual Resource on the Master NGFW Engine to which you want to add the Virtual Firewall.

5) (Optional) In the **DNS IP Addresses** field, add one or more IP addresses of DNS servers that the Virtual Firewall uses to resolve domain names. There are two ways to define IP addresses.
   - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog box that opens.
   - To define an IP address using a network element, click **Add** and select **Network Element**.

6) (Optional) Next to the **Category** field, click **Select** and select one or more categories.

7) Click **Save**.
   Do not close the Engine Editor.

Next steps

Configure interfaces for the Virtual Layer 2 Firewall.

Configuring Physical Interfaces for Virtual Layer 2 Firewalls

Physical interfaces for Virtual Layer 2 Firewalls represent interfaces allocated to the Virtual Layer 2 Firewall in the Master NGFW Engine.

When you select the Virtual Resource for the Virtual Layer 2 Firewall, physical interfaces are automatically created based on the interface configuration of the Master NGFW Engine. The number of physical interfaces depends on the number of interfaces allocated to the Virtual Layer 2 Firewall in the Master NGFW Engine. It is not recommended to create new physical interfaces in the Virtual Layer 2 Firewall properties, as they might not be valid.

You can optionally change the automatically created physical interfaces in the Virtual Layer 2 Firewall properties. For detailed instructions, see the *Forcepoint Next Generation Firewall Product Guide*.

Add VLAN interfaces to Virtual NGFW Engine interfaces

VLANs divide a single physical network link into several virtual links.

VLAN interfaces can only be added for Virtual NGFW Engines if the creation of VLAN interfaces for Virtual Firewalls is enabled in the Master NGFW Engine Properties. The maximum number of VLANs for a single physical interface is 4094. The VLANs must also be defined in the configuration of the external switch or router to which the interface is connected.

Note

You cannot add VLAN interfaces on top of other VLAN interfaces. Depending on the configuration of the Master NGFW Engine, you might not be able to create valid VLAN interfaces for the Virtual NGFW Engine. Contact the administrator who configured the Master NGFW Engine.

Steps

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

1) Right-click a Virtual Firewall, Virtual IPS engine, or Virtual Layer 2 Firewall and select **Edit <element type>**.
2) In the navigation pane on the left, select **Interfaces**.
3) Right-click a physical interface and select **New** > **VLAN Interface**.
4) Define the VLAN interface properties.

   CAUTION

   The throughput for the Virtual Firewall physical interface must not be higher than the throughput for the Master NGFW Engine interface that hosts the Virtual Firewall. Contact the administrator of the Master NGFW Engine before changing this setting.

   CAUTION

   Make sure that you set the interface speed correctly. When the bandwidth is set, the Virtual NGFW Engine always scales the total amount of traffic on this interface to the bandwidth you defined. The bandwidth is scaled even if there are no bandwidth limits or guarantees defined for any traffic.

5) Click **OK**.
   The specified VLAN ID is added to the physical interface.

Next steps

Continue the configuration in one of the following ways:

- (Virtual Firewall only) If you do not want to add tunnel interfaces for a route-based VPN, add IP addresses directly to the physical interfaces.
- Otherwise, click **Save and Refresh** to transfer the configuration changes.

Chapter 9

Configuring routing

Contents

After creating the NGFW Engine elements and defining the interfaces, you can configure the basic routing.

Getting started with routing

Routes to directly connected networks are automatically added according to the interfaces defined for each NGFW Engine. You must manually add other routes or configure dynamic routing.

When the NGFW Engine reads routing definitions, it selects the most specific route and antispoofing definition it finds for each packet. The NGFW Engine:

1) Checks if there is a route defined for the specific destination IP address of the packet (Host elements).

2) Checks routes to the defined networks (Network elements).

3) Uses the default route (the Any network element) if no other route matches the packet's destination address. The default route typically leads to the Internet if the site has Internet access.

If there are overlapping definitions, the more specific one is considered first.

Firewalls

You must add the default route and routes through next-hop gateways to networks that are not directly connected to the NGFW Engine.

IPS engines and Layer 2 Firewalls

The routing information for IPS engines and Layer 2 Firewalls is only used for system communications. The inspected traffic is not routed. Inline interfaces are always fixed as port pairs: traffic that enters through one port is automatically forwarded to the other port. For NGFW Engines in the IPS and Layer 2 Firewall roles, you only need to add a default route or additional routes if one or more SMC components are not directly connected and cannot be reached through the default gateway. If needed, you can add the default route and routes to internal networks that are not directly connected to the IPS or Layer 2 Firewall if the networks cannot be reached through the default gateway.

Master NGFW Engines and Virtual NGFW Engines

Master NGFW Engines proxy all communication between Virtual NGFW Engines and other SMC components. You do not need to configure routing for Virtual Firewalls, Virtual IPS engines, or Virtual Layer 2 Firewalls in order for them to be managed by the SMC.

Antispoofing

Spoofing an IP address means using the IP address of a legitimate (internal) host to gain access to protected resources. The antispoofing configuration is automatically generated based on the routing information of NGFW Engines. By default, connection attempts with a source IP address from a certain internal network are only allowed through if they are coming from the correct interface as defined in the routing configuration. As the routing entry is needed for the communications to work, antispoofing rarely needs additional modifications. For more information, see the *Forcepoint Next Generation Firewall Product Guide*.

Elements used to configure routing

- Network elements represent a group of IP addresses.
- Router elements represent next-hop routers.
- NetLink elements are used for configuring Multi-Link routing. For more information, see the *Forcepoint Next Generation Firewall Product Guide*.

When interfaces are aggregated as one interface, those interfaces work together as a single interface. For aggregated interfaces in load-balancing mode, make sure that the connected switch supports the link aggregation control protocol (LACP), and that LACP is configured on the switch.

Add routers

A Router element represents a next-hop gateway's IP address in routing configurations.

Steps

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

1) Select **Configuration**.
2) Right-click an NGFW Engine, then select **Edit <element type>**.
3) Browse to **Routing**.
4) Right-click a Network element that is beneath an interface, then select **Add Router**.
5) Select **Tools** > **New** > **Router**.
6) Enter a name and the IP address of the router, then click **OK**.
7) Select the Router you created, then select **Add**.

8) Click **OK**.

9) Click **Save**.

Add or view the default route

You can check which route is currently set as the default route for traffic leaving the NGFW Engine and set a new default route.

Steps

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

1) Select **Configuration**.

2) Right-click an NGFW Engine, then select **Edit <element type>**.

3) Browse to **Routing**.

Tip

To view the full routing information for all interfaces, click **Expand All**.

4) To show the default route, click **Show Default Route** in the **Routing Tools** pane.
The current default route or routes are shown in bold font.

5) To set the default route, right-click a router or NetLink, then select **Set as Default Route**.
The Any network element is added beneath the router and is set as the default route.

6) Click **Save and Refresh**.

Add static routes

You can add a static route to a network in the routing configuration.

Steps

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

1) Select **Configuration**.

2) Right-click an NGFW Engine, then select **Edit <element type>**.

3) Browse to **Routing**.

Tip

To view the full routing information for all interfaces, click **Expand All**.

4) Right-click the router or NetLink through which you want to route traffic, select **Add**, then select a Network element.

   For a route through a tunnel interface, add the Network element directly to the tunnel interface.

5) Click **Save and Refresh**.

Chapter 10

Initial configuration of Forcepoint NGFW software

Contents

After configuring the NGFW Engines in the Management Client, apply the initial configuration of the NGFW Engine and contact the Management Server.

Options for initial configuration

You can configure the Forcepoint NGFW software using plug-and-play configuration, automatic configuration, or the NGFW Configuration Wizard.

Forcepoint NGFW appliances come with Forcepoint NGFW software installed. If you have an NGFW Engine license, you can configure the engine in any of the three NGFW Engine roles. If you have a license for a specific type of engine (Firewall/VPN or IPS), you can only use the engine in that specific role.

There are three ways to configure the Forcepoint NGFW software.

- **Plug-and-play configuration** — The Forcepoint NGFW appliance automatically connects to the Installation Server, downloads the initial configuration file, then contacts the Management Server.
  You must have Forcepoint NGFW appliances and proof-of-serial codes to use plug-and-play configuration. Plug-and-play configuration is only supported for single NGFW Engines in the Firewall/VPN role that have a dynamic control IP address.

  Note

  There are special considerations when using plug-and-play configuration. For example, both the SMC and the NGFW Engines must be registered for plug-and-play configuration before you configure the engines. See Knowledge Base article 9662.

- **Automatic configuration** — You can configure Forcepoint NGFW appliances automatically with a USB drive that contains the initial configuration files.
- **NGFW Configuration Wizard** — If it is not possible to use plug-and-play configuration or automatic configuration, or you do not want to use them, you can use the NGFW Configuration Wizard. You can use the NGFW Configuration Wizard in two ways:
  - Connect a serial cable to the appliance and use the NGFW Configuration Wizard on the command line.
  - Connect an Ethernet cable to the appliance and use the NGFW Configuration Wizard in a web browser.

Before a policy can be installed on the appliance, you must configure some permanent and some temporary network settings for the engine.

To successfully complete the initial configuration:

1) The SMC must be installed.

2) The NGFW Engine elements (Firewall, IPS, or Layer 2 Firewall elements) must be defined in the Management Client.

3) Engine-specific configuration information must be available from the Management Server. The required information depends on the configuration method.
   - For plug-and-play configuration, the initial configuration file for the NGFW Engine must be uploaded to the Installation Server.
   - For automatic configuration, you must have saved the initial configuration file on a USB drive.
   - For the NGFW Configuration Wizard, you must have a one-time password for the engine.

The appliance must contact the Management Server before it can be operational.

Using plug-and-play configuration

In plug-and-play configuration, the Forcepoint NGFW appliance automatically connects to the Installation Server, downloads the initial configuration file, then contacts the Management Server.

Prepare for plug-and-play configuration

To use plug-and-play-configuration, save the initial configuration file, then upload it to the Installation Server.

Steps

1) Register the SMC and NGFW for plug-and-play configuration.
   a) Go to https://stonesoftlicenses.forcepoint.com.
   b) In the **License Identification** field, enter your SMC POL code, then click **Submit**.
   c) Click **Register your appliances for Plug & Play installation on NGFW Installation Cloud**.
   d) Enter your NGFW appliance POS codes and your contact information, then click **Submit**.

2) In the Management Client, select **Configuration**.

3) Right-click the NGFW Engine for which you want to save the initial configuration, then select **Configuration** > **Save Initial Configuration**.

4) (Optional) If you already have a policy you want to use for the engine, click **Select**, then select a policy as the initial security policy.
   The selected policy is automatically installed after the NGFW Engine has contacted the Management Server.

5) (Optional) Select **Enable SSH Daemon** to allow remote access to the NGFW Engine command line.
   - Enabling SSH in the initial configuration gives you remote command-line access in case the configuration is imported correctly, but the engine fails to establish contact with the Management Server.
   - After the NGFW Engine is fully configured, you can enable or disable SSH access using the Management Client. We recommend that you enable SSH access in the Management Client when needed and disable the access again when you are finished. Make sure that your Access rules allow SSH access to the engines from the administrators' IP addresses only.

   CAUTION

   If you enable SSH, set the password for command-line access after the initial configuration either through the Management Client or by logging on to the command line. When the password is not set, anyone with SSH access to the engine can set the password.

6) From the **Local Time Zone** drop-down list, select the time zone.

   The time zone selection is used only for converting the UTC time that the engines use internally for display on the command line. All internal operations use UTC time, which is synchronized with the Management Server's time after the engine is configured. For external operations, engines use the time zone of their geographical location.

7) From the **Keyboard Layout** drop-down list, select the keyboard layout used for the engine command line.

8) Select **Upload to Installation Server** to upload the initial configuration file automatically to the Installation Server.

9) Click **Close**.

Next steps

Configure the Forcepoint NGFW software using plug-and-play configuration.

Configure Forcepoint NGFW software using plug-and-play configuration

Connect the Forcepoint NGFW to the network to start the plug-and-play configuration.

Before you begin

The SMC and NGFW Engine must be registered for plug-and-play configuration.

The initial configuration file for the NGFW Engine must be uploaded to the Installation Server.

The Forcepoint NGFW appliance uses specific ports in a specific order when it tries to connect to the Installation Server.

Note

Use these default port settings in the properties of the corresponding engine interfaces that you have defined in the Management Client. The initial configuration fails if the port settings on the physical appliance and the interface definitions in the engine element properties are not the same.

The Forcepoint NGFW appliance first tries to contact the Installation Server through the mobile broadband modem if one is connected to a USB port. The mobile broadband modem and the corresponding Modem interface in the Management Client must have the following settings:

- **Access Point Name** — internet
- **Phone number** — *99#
- **PIN Code** — <empty value>

Note

PIN code must also be disabled on the mobile broadband modem.

If attempts to connect to the Installation Server through the mobile broadband modem fail, the appliance tries to connect to the Installation Server through Ethernet port 0. If no mobile broadband modem is connected to the appliance, Ethernet port 0 is the only port that can be used.

Steps

1) (Optional) If you want to view the progress of the plug-and-play configuration, connect the appliance to a computer using the serial cable supplied with the appliance, and use a terminal console program to connect to the NGFW appliance with these settings:
   - **Bits per second** — 115,200
   - **Data bits** — 8
   - **Parity** — None
   - **Stop bits** — 1.

   Note

   The serial console port speed is 115,200 bps in most NGFW appliances. The speed is 9600 bps in older NGFW appliance models. See the hardware guide for your NGFW appliance model for more information.

2) (Optional) Plug an empty USB drive into one of the USB ports on the appliance if you want to save information about the progress of the plug-and-play configuration on a USB drive.

   Saving the progress information on a USB drive can be useful, for example, for troubleshooting purposes.

3) Connect the network cables to the appliance. On specific Forcepoint NGFW appliance models with wireless support, connect the antennas.

   Note

   The wireless port on Forcepoint NGFW appliances cannot be used for connecting to the Installation Server.

4) Turn on the NGFW appliance.

Result

The appliance automatically contacts the Installation Server. When the contact succeeds, the appliance downloads the initial configuration file from the Installation Server, then contacts the Management Server.

If plug-and-play configuration fails

If the plug-and-play configuration fails, check for possible causes and solutions.

Note

There are special considerations when using plug-and-play configuration. For example, both the SMC and the NGFW Engines must be registered for plug-and-play configuration before you configure the engines. See Knowledge Base article 9662.

If you plugged in a USB drive to the appliance, check the sg_autoconfig.log file on the USB drive.

If you see a connection refused error message, make sure that the Management Server IP address is reachable from the engine. Also check the settings that you have defined for the engine's interfaces in the Management Client. The port numbers and settings must match the interface IDs and other interface settings in the Management Client.

If attempts to connect to the Installation Server through the mobile broadband modem and Ethernet port 0 have failed, the appliance starts the connecting process again. It retries the ports in the same order (mobile broadband modem, then Ethernet port 0). If necessary, you can run the command `sg-reconfigure --stop-autocontact` on the engine command line to stop this process.

If plug-and play-configuration continues to fail, save the initial configuration file on a USB drive, then configure the engine using the automatic configuration method.

Using automatic configuration

In automatic configuration, you configure the engine automatically using a USB drive that contains the initial configuration files.

Prepare for automatic configuration

To use automatic configuration, save the initial configuration files on a USB drive.

When you save the initial configuration for an NGFW Engine cluster, the Management Server generates initial configuration files for all nodes at the same time. You can save all the initial configuration files on the same USB drive. When you apply the initial configuration to individual nodes, each node uses the initial configuration files on the USB drive in order.

Note

If you are configuring multiple NGFW Engine clusters, you must save the initial configuration files for each cluster on a separate USB drive.

Steps

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

1) In the Management Client, select **Configuration**.

2) Right-click the NGFW Engine for which you want to save the initial configuration, then select **Configuration** > **Save Initial Configuration**.

3) (Optional) If you already have a policy you want to use for the engine, click **Select**, then select a policy as the initial security policy.

   The selected policy is automatically installed on the engine after the engine has contacted the Management Server.

4) From the **Local Time Zone** drop-down list, select the time zone.

   The time zone selection is used only for converting the UTC time that the engines use internally for display on the command line. All internal operations use UTC time, which is synchronized with the Management Server's time after the engine is configured. For external operations, engines use the time zone of their geographical location.

5) From the **Keyboard Layout** drop-down list, select the keyboard layout used for the engine command line.

6) (Optional) Select **Enable SSH Daemon** to allow remote access to the engine command line.

   - Enabling SSH in the initial configuration gives you remote command-line access in case the configuration is imported correctly, but the engine fails to establish contact with the Management Server.
   - After the engine is fully configured, you can set SSH access on or off using the Management Client. We recommend that you enable the SSH access in the Management Client when needed and disable the access again when you are finished. Make sure that your access rules allow SSH access to the engines from the administrators' IP addresses only.

   CAUTION

   If you enable SSH, set the password for command-line access after the initial configuration either through the Management Client or by logging on to the command line. When the password is not set, anyone with SSH access to the engine can set the password.

7) Click **Save As**, then save the configuration file or files to the root directory of a USB drive.

   Do not change the default file name. Use a separate USB drive for each single NGFW Engine or NGFW Engine cluster.

   CAUTION

   Handle the configuration files securely. They include the one-time password that allows establishing trust with your Management Server.

8) Click **Close**.

Next steps

Configure the Forcepoint NGFW software using automatic configuration.

Configure Forcepoint NGFW software using automatic configuration

Automatic configuration is primarily intended to be used with Forcepoint NGFW appliances, and might not work in all environments when you use your own hardware.

Before you begin

Connect a network cable to the interface that you have configured as the control interface.

If the automatic configuration does not work, use the NGFW Configuration Wizard and import or enter the information manually.

When automatic configuration is used, Interface IDs are mapped to network interfaces on the engine in sequential order: Physical Interface ID 0 is mapped to eth0, Physical Interface ID 1 is mapped to eth1, and so forth.

Note

The imported configuration does not contain a password for the root account. You must set the password after the configuration has been successfully completed.

Steps

1) Make sure that you have a physical connection to the NGFW appliance using a monitor and keyboard or a serial cable.

   If you use a serial cable, use a terminal console program to connect to the NGFW appliance with these settings:

   - **Bits per second** — 115,200
   - **Data bits** — 8
   - **Parity** — None
   - **Stop bits** — 1.

   Note

   The serial console port speed is 115,200 bps in most NGFW appliances. The speed is 9600 bps in older NGFW appliance models. See the hardware guide for your NGFW appliance model for more information.

2) Insert the USB drive, then turn on the NGFW appliance.

   The NGFW appliance starts, applies the initial configuration file that is saved on the USB drive, then makes initial contact to the Management Server.

   - If the automatic configuration fails, and you do not have a monitor connected, check sg_autoconfig.log on the USB drive.
   - If you see a connection refused error message, make sure that the Management Server IP address is reachable from the node.

3) When you see the prompt that indicates that the installation is finished, remove the USB drive, then press **Enter**.

   The console opens and you are prompted to set the password for the root account.

4) Enter and confirm the password.

Result

When the appliance successfully contacts the Management Server, the configuration is complete.

Using the NGFW Configuration Wizard

You can import or manually configure the settings for the NGFW Engine using either the command line or the web browser version of the NGFW Configuration Wizard.

There are some limitations for the web browser version of the NGFW Configuration Wizard.

- Only IPv4 addresses are supported.
- You must configure the SMC to use 256-bit security for communications.
- You cannot connect the appliance to the network through a mobile broadband modem.
- You cannot configure PPPoA interfaces.
- You cannot make the appliance follow FIPS 140-2 standards.

Note

After completing the web browser version of the NGFW Configuration Wizard, to make any changes to the configuration, you must start the configuration from the beginning. If you only want to make minor changes to the configuration, use the command-line version of the NGFW Configuration Wizard.

Prepare for NGFW Configuration Wizard configuration

To use the NGFW Configuration Wizard, save the initial configuration file or write down the configuration information for manual configuration.

Steps

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

1) In the Management Client, select **Configuration**.

2) Right-click the engine for which you want to save the initial configuration, then select **Configuration** > **Save Initial Configuration**.

3) To see the one-time passwords and fingerprints, click **View Details**.
   If you plan to import the configuration information, you do not need to write down or copy these details.
   a) From the **One-Time Password** field, write down or copy the one-time password for each engine node.
   Make a note of which password belongs to which engine node.

b) From the **Management Server Addresses** field, write down or copy the IP addresses of the Management Server.

c) (Optional) From the **Management Server Certificate Fingerprint (MD5)** or **Management Server Certificate Fingerprint (SHA-512)** field, write down or copy the fingerprint of the Management Server's certificate.

d) Click **Close**.

4) Select the other configuration options.

a) (Optional) If you already have a policy you want to use for the engine, click **Select**, then select a policy.

The selected policy is automatically installed on the engine after the engine has contacted the Management Server.

b) From the **Local Time Zone** drop-down list, select the time zone.

The time zone selection is used only for converting the UTC time that the engines use internally for display on the command line. All internal operations use UTC time, which is synchronized with the Management Server's time once the engine is configured. For external operations, engines use the time zone of their geographical location.

c) From the **Keyboard Layout** drop-down list, select the keyboard layout used for the engine command line.

d) Select **Enable SSH Daemon** to allow remote access to the engine command line.

Enabling SSH in the initial configuration gives you remote command-line access in case the configuration is imported correctly, but the engine fails to establish contact with the Management Server. After the engine is fully configured, you can set SSH access on or off using the Management Client. We recommend that you enable the SSH access in the Management Client when needed and disable the access again when you are finished. Make sure that your Access rules allow SSH access to the engines from the administrators' IP addresses only.

CAUTION

If you enable SSH, set the password for command-line access after the initial configuration either through the Management Client or by logging on to the command line. When the password is not set, anyone with SSH access to the engine can set the password.

e) Under **Manual Installation**, click **Save As**, then save the configuration file.

CAUTION

Handle the configuration files securely. They include the one-time password that allows establishing trust with your Management Server.

Tip

Keep the **Save or Upload Initial Configuration** dialog box open while you configure the Forcepoint NGFW software.

Next steps

Start the NGFW Configuration Wizard.

Start the NGFW Configuration Wizard on the command line

Start the NGFW Configuration Wizard to configure settings for the Forcepoint NGFW engine.

Tip

You can run the NGFW Configuration Wizard at any time using the `sg-reconfigure` command on the engine command line.

Steps

1) If you are configuring a physical device, connect to the Forcepoint NGFW appliance.
   a) Connect the Forcepoint NGFW appliance to a laptop or other client device using a serial cable.
   b) On the client device, use a terminal console program to connect to the NGFW appliance with these settings:
      - **Bits per second** — 115,200
      - **Data bits** — 8
      - **Parity** — None
      - **Stop bits** — 1.

      Note

      The serial console port speed is 115,200 bps in most NGFW appliances. The speed is 9600 bps in older NGFW appliance models. See the hardware guide for your NGFW appliance model for more information.

   c) Connect the network cables to the Forcepoint NGFW appliance.
2) Turn on the Forcepoint NGFW appliance.
3) Start the NGFW Configuration Wizard.

   Note

   On some appliance models, the NGFW Configuration Wizard starts automatically.

   a) Press **Enter** to activate the console.
   b) When you are prompted to start the NGFW Configuration Wizard, type `Y`, then press **Enter**.

4) Select the role for the NGFW Engine.

   If you have an NGFW Engine license, you can select any of the NGFW Engine roles. The role must correspond to the engine element (Firewall, Layer 2 Firewall, or IPS) that you defined in the Management Client. You can later change the engine's role. If you have a license for a specific type of engine (Firewall/VPN or IPS), select the role that corresponds to the type of license you have.

   a) Highlight **Role**, then press **Enter**.

   b) Highlight **Firewall**, **IPS**, or **Layer 2 Firewall**, then press **Enter**.

5) Select one of the following configuration methods:
   - Highlight **Import**, then press **Enter** to import a saved configuration.
   - Highlight **Next**, then press **Enter** to manually configure the engine's settings.

6) If you have stored the configuration on a USB drive, import the configuration.

   a) Select **USB Memory**, then press **Enter**.

   b) Select the correct configuration file.

   The files are specific to each engine node.

   c) Highlight **Next**, then press **Enter**.

Configure general settings on the command line

The settings include console keyboard layout, time zone, and other optional settings.

Some of the settings might be filled in if you imported the configuration from a USB drive.

Steps

1) Set the console keyboard layout.

   a) Highlight the entry field for **Keyboard Layout**, then press **Enter**.

   b) Highlight the correct layout, then press **Enter**.

   The keyboard layout setting only applies to hardware that you connect to using a directly connected keyboard and monitor. This setting has no effect if you connect to the appliance through the serial console port or over the network using SSH.

   If the keyboard layout that you want to use is not listed, select the best-matching available layout or select **US_English**.

   Tip

   Type the first letter of the keyboard layout to skip ahead in the list.

2) Set the time zone.

   a) Highlight the entry field for **Local Timezone**, then press **Enter**.

b) Select the time zone from the list.

The time zone setting affects only the way the time is displayed on the engine command line. The actual operation always uses UTC time. The engine's clock is automatically synchronized with the Management Server's clock.

3) Set the rest of the settings.

a) Enter the host name of the engine.

b) Enter and confirm the password for the root user account.

This account is the only one with command-line access to the engine.

c) (Optional) Highlight **Enable SSH Daemon**, then press the spacebar to allow remote access to the engine command line using SSH.

Note

Unless you have a specific reason to enable SSH access to the engine command line, we recommend leaving it disabled.

d) (Optional) If you are required to follow the FIPS 140-2 standards, select **Restricted FIPS-Compatible Operating Mode**.

Note

This option only is for environments that are required to follow the FIPS 140-2 standards. Do not select this option unless you have a specific reason to do so.

e) (Optional) Enter and confirm a bootloader password.

If you configure a bootloader password, you must enter the bootloader password to edit the options that appear in the bootloader menu of the NGFW appliance.

f) Highlight **Next**, then press **Enter**.

Configure network interfaces on the command line

The NGFW Configuration Wizard can automatically detect which network cards are in use. You can also add interfaces manually.

Steps

1) Define the network interface drivers.

If the list is not populated automatically, use auto-detect.

a) Highlight **Autodetect**, then press **Enter**.

b) Check that the autodetected information is correct and that all interfaces have been detected.

Tip

You can use the Sniff option for troubleshooting the network interfaces. Select **Sniff** to run a network sniffer on that interface.

If autodetection fails, add network drivers manually.

a) Highlight **Add**, then press **Enter**.

b) Select the correct driver for your network card, then press **Enter**.

2) Map interfaces to the IDs you defined.

a) Change the IDs as necessary to define how the interfaces are mapped to the interface IDs you defined for the engine element in the Management Client.

For bypass interface modules, map the interface IDs of inline interfaces to even-odd pairs of ports on the appliance. For example, map Interface ID 1 to port eth2_0 and Interface ID 2 to port eth2_1.

b) If necessary, highlight the **Media** column, then press **Enter** to change the settings to match those used by the device at the other end of the link.

Make sure that the speed/duplex settings of network cards are identical at both ends of each cable. For IPS and Layer 2 Firewall engines, also make sure that the speed/duplex settings of the inline interfaces match the speed/duplex settings of both links within each inline interface pair.

c) In the **Mgmt** column, highlight the correct interface for contact with the Management Server, then press the spacebar.

Important

The Management interface must be the same interface on which the control IP address for the corresponding element is configured in the SMC.

d) (Optional, IPS only) Highlight **Initial Bypass**, then press **Enter** to temporarily set the IPS engine to the initial bypass state and define one or more soft-bypass interface pairs through which traffic flows.

Setting the appliance to the initial bypass state can be useful during IPS appliance deployment if bypass network interface pairs on the appliance are in Normal mode. Initial bypass allows traffic to flow through the IPS appliance until the initial configuration is ready and an IPS policy is installed on the appliance. Do not set the initial bypass state when the bypass network interface pairs are in Bypass mode.

3) (Modem interfaces only) Map the modem number to the IMEI of the modem.

a) Select **Setup modems**.

The first modem number is automatically mapped to the IMEI of the modem. You can optionally change the modem number.

b) Select **Stored**, then select **OK**.

Contact the Management Server on the command line

Provide the necessary information to allow the NGFW Engine to establish contact with the Management Server.

Before the engine can make initial contact with the Management Server, you activate the initial configuration on the engine. The initial configuration contains the information that the engine requires to connect to the Management Server for the first time.

If the initial configuration was imported from a USB drive, most of the options on the **Prepare for Management Contact** page are filled in.

Important

If there is a firewall between this engine and the Management Server, make sure that the intermediate firewall's policy allows the initial contact and all subsequent communications.

Steps

1) If the control IP address is dynamic, select **DHCPv4**, **SLAAC (IPv6)**, or **DHCPv6**.

   Note

   The same protocol must be selected in the IP address properties in the Management Client.

2) If the NGFW Engine uses PPP for management contact, define the PPP settings.
   a) Highlight **Settings**, then press **Enter**.
   b) On the **PPP Settings** page, fill in the account details according to the information you have received from your service provider.
   c) Highlight **OK**, then press **Enter**.

3) If the NGFW Engine uses a modem for management contact, define the modem settings.
   a) Highlight **Settings**, then press **Enter**.
   b) On the **Modem Settings** page, enter the PIN code, then select **OK**.
      The same PIN code must be configured in the properties of the modem interface in the Management Client.
   c) Highlight **OK**, then press **Enter**.

4) If the control IP address is static, select **Enter node IP address manually**, then define the IP address of the Forcepoint NGFW node.
   a) In the **IP Address** field, enter the IP address.
   b) In the **Netmask/Prefix Length** field, enter the netmask (IPv4) or prefix length (IPv6) of the network.

c) If the Management Server is not in a directly connected network, enter the IP address of the next-hop gateway in the **Gateway to management** field.

5) If the control IP address is on a VLAN interface, select **Use VLAN, Identifier**, then enter the VLAN ID.

6) Select **Contact** or **Contact at Reboot**, then press the spacebar.

7) Enter the Management Server IP address and the one-time password.

Note

The one-time password is engine-specific and can be used only for one initial connection to the Management Server. After initial contact has been made, the engine receives a certificate from the SMC for identification. If the certificate is deleted or expires, repeat the initial contact using a new one-time password.

8) (Optional) To use 256-bit encryption for the connection to the Management Server, select **256-bit Security Strength**, then press the spacebar.

Note

256-bit encryption must also be enabled for the Management Server in the SMC.

9) (Optional) Highlight **Edit Fingerprint**, then press **Enter**. Fill in the Management Server's certificate fingerprint (also shown when you saved the initial configuration).

Filling in the certificate fingerprint increases the security of the communications.

10) Highlight **Finish**, then press **Enter**.

The engine now tries to make initial contact with the Management Server. The progress is displayed on the command line. If you see a connection refused message, make sure that the one-time password is correct and the Management Server IP address is reachable from the node. Save a new initial configuration if you are unsure about the password.

Note

If the initial management contact fails for any reason, you can start the configuration again with the `sg-reconfigure` command.

Result

After you see notification that Management Server contact has succeeded, the engine installation is complete and the engine is ready to receive a policy.
The engine element's status changes in the Management Client from **Unknown** to **No Policy Installed**. The connection state is **Connected**, indicating that the Management Server can connect to the node.

Next steps

Install a policy on the engine using the Management Client

Related information
Default communication ports on page 235

Start the NGFW Configuration Wizard in a web browser

Start the NGFW Configuration Wizard to configure settings for the Forcepoint NGFW engine.

Steps

1) If you are configuring a physical Forcepoint NGFW appliance, connect the appliance to a laptop or other client device.
   a) Connect an Ethernet cable from the client device to physical port eth0_1 on the NGFW appliance.
      If the NGFW appliance does not have a port eth0_1, use port eth1_0. If using non-modular interfaces, use port eth1.
   b) Connect the other network cables to the Forcepoint NGFW appliance.
2) Turn on the Forcepoint NGFW appliance.
3) To start the web browser version of the NGFW Configuration Wizard, open a web browser on the client device, then connect to https://169.254.169.169.
   It might take some time for the web page to load.
4) When the NGFW Configuration Wizard offers a web browser client certificate, accept the certificate.

Configure general settings in a web browser

The settings include keyboard layout, timezone, and other optional settings.

Steps

1) On the **Welcome** screen, select **Start**.
2) Select **I agree to the terms and conditions**, then select **Next**.
3) Enter and confirm a password for the root user account, then select **Next**.
4) Select the configuration method, then select **Next**.
   - If you have a .cfg configuration file, select **Import**.
   - If you want to enter the settings manually, select **Manual**.
5) If you selected **Import**, import the .cfg configuration file.
   a) Select **Select File**, browse for the .cfg configuration file, then select the file.
   b) Select **Import Configuration**.
   c) After the file has been imported, select **Next**.

6) If you selected **Manual** as the configuration method, select the role for the NGFW Engine, then select **Next**.

7) On the **Basic Information** screen, enter the required information, then select **Next**.

Note

If you imported a configuration file, some of the information might be filled in automatically.

a) Enter the host name for the appliance.

b) Select the time zone to use on the appliance.

The time zone setting affects only the way the time is displayed on the engine command line. The actual operation always uses UTC time. The engine's clock is automatically synchronized with the Management Server's clock.

c) Select the keyboard layout to use when working on the command line of the engine.

The keyboard layout setting only applies to hardware that you connect to using a directly connected keyboard and monitor. This setting has no effect if you connect to the appliance through the serial console port or over the network using SSH.

d) To allow connections to the engine using SSH, select **Enable SSH Access**.

Note

Unless you have a specific reason to enable SSH access to the engine command line, we recommend leaving it disabled.

Configure network interfaces in a web browser

The NGFW Configuration Wizard can automatically detect which network cards are in use.

Note

If you imported a configuration file, the information is filled in automatically.

Steps

1) To change the mapping of the interface IDs, select **Change the Mapping**.

a) Change the IDs as necessary to define how the interfaces are mapped to the interface IDs that you defined for the engine element in the Management Client.

For bypass interface modules, map the interface IDs of inline interfaces to even-odd pairs of ports on the appliance. For example, map Interface ID 1 to port eth2_0 and Interface ID 2 to port eth2_1.

b) If necessary, select the **Speed/Duplex** column to change the settings to match those used by the device at the other end of the link.

Make sure that the speed/duplex settings of network cards are identical at both ends of each cable. For IPS and Layer 2 Firewall engines, also make sure that the speed/duplex settings of the inline interfaces match the speed/duplex settings of both links within each inline interface pair.

2) (Modem interfaces only) Map the modem number to the IMEI of the modem.

   a) Select **Setup modems**.

      The first modem number is automatically mapped to the IMEI of the modem. You can optionally change the modem number.

   b) Select **Stored**, then select **OK**.

3) Select **Save**, then select **Next**.

4) Select the interface to use for management connectivity.

   The Management interface must be the same interface on which the control IP address for the corresponding element is configured in the SMC.

5) If the Management interface is on a VLAN interface, enter the VLAN ID.

6) Set the interface type.

   - If the interface is a dynamic interface that receives its IP address from a DHCP Server, select **Dynamic IPv4 Address (DHCP)**.
   - If the interface is dynamic interface that receives its IP address from a PPPoE Server, select **Dynamic IPv4 Address (PPPoE Server)**, select **PPPoE Settings**, then fill in the account details according to the information you have received from your service provider.
   - If the interface is a static interface, select **Static**, then enter the IP address and netmask.

7) Select **Next**.

8) Enter the IP address of the Management Server.

9) If the Management Server is not located in a directly-connected network, enter the IP address of the next-hop gateway in the **Default Gateway** field.

10) Select **Next**.

Contact the Management Server in a web browser

Provide the necessary information to allow the NGFW Engine to establish contact with the Management Server.

Note

If you imported a configuration file, the information is filled in automatically.

Important

If there is a firewall between this engine and the Management Server, make sure that the intermediate firewall's policy allows the initial contact and all subsequent communications.

Steps

1) Select when you want the appliance to make contact with the Management Server.
   - **At the end of this session** — The appliance makes contact after you confirm the entered information.
   - **After the appliance restarts** — The appliance makes contact after you confirm the entered information and the appliance restarts.

2) Enter the one-time password generated by the SMC.

   Note

   The one-time password is engine-specific and can be used only for one initial connection to the Management Server. After initial contact has been made, the engine receives a certificate from the SMC for identification. If the certificate is deleted or expires, repeat the initial contact using a new one-time password.

3) (Optional if you set the appliance to attempt to make contact at the end of this session) Enter the SHA-512 fingerprint generated by the SMC.

   Filling in the certificate fingerprint increases the security of the communications.

4) If the NGFW Engine uses a modem for management contact, define the modem settings.
   a) Highlight **Settings**, then press **Enter**.
   b) On the **Modem Settings** page, enter the PIN code, then select **OK**.

      The same PIN code must be configured in the properties of the modem interface in the Management Client.
   c) Highlight **OK**, then press **Enter**.

5) Select **Next**.

6) Review the configuration summary, then continue the configuration in one of the following ways:
   - If you set the initial contact to be made at the end of this session, select **Finish and Contact the Management Server**.
   - If you set the initial contact to be made after the appliance restarts, select **Apply Configuration and Finish**.

7) If you set the initial contact to be made after the appliance restarts, after the configuration has been applied, select **Finish and Turn Off**.

   When you turn the appliance back on, the appliance makes the initial contact.

8) If you set the initial contact to be made at the end of this session, and if you did not previously enter the SHA-512 fingerprint generated by the SMC, verify that the fingerprint shown matches, then select **Finish and Proceed**.

   Note

   If you do not select **Finish and Proceed** within the timeout, the **Reject** option is used, and you must make the initial contact again.

Result

After the initial contact has been made successfully, the NGFW Configuration Wizard shuts down and the Ethernet port used to connect to the appliance is released for regular use.
If you set the initial contact to be made at the end of this session, a notification is shown in the web browser. If you set the initial contact to be made after the appliance restarts, the notification is not shown.

The engine element's status changes in the Management Client from **Unknown** to **No Policy Installed**. The connection state is **Connected**, indicating that the Management Server can connect to the node.

Note

If the status remains **Unknown**, run the NGFW Configuration Wizard again, and review the settings. All settings can be changed, except for the engine role. To change the engine role, you must first reset the appliance to factory default settings.

Next steps

After the appliance has been configured, install a policy on the engine using the Management Client.

Troubleshoot using the NGFW Configuration Wizard in a web browser

If you are unable to make contact with the Management Server, you can generate an sgInfo file to send to Forcepoint support, or you can reset the appliance to factory default settings and try configuring the appliance again.

Steps

1) Generate an sgInfo file that contains information for Forcepoint support to use.
   a) In the top right corner of the screen, select ⚙ > **Information for support**.
   b) Select **Get Information for support**.
   c) Select **Download**, then save the sginfo.tar.gz file to your client device.
2) Reset the appliance to factory default settings.
   a) In the top right corner of the screen, select ⚙ > **Reset to factory default settings**.

      Note

      This option is available only after you get to the **Configuration Method** screen.

   b) Select **Confirm Reset**.

      Note

      You do not receive confirmation that the reset has completed.

Chapter 11

Creating and installing policies

Contents

After successfully applying the initial configuration and establishing contact between the NGFW Engines and the Management Server, the NGFW Engine is in the initial configuration state. Now you can create and install policies for access control or inspecting traffic.

In addition to the rules in the policy, other configuration information, such as interface definitions and routing information, is also transferred to the NGFW Engine when you install a policy.

Create and install a Firewall Policy

Create a basic policy for firewalls.

Steps

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

1) Select **Configuration**.

2) Right-click **Policies**, then select **New** > **Firewall Policy**.

3) Enter a name for the Policy.

4) Select **Firewall Template** as the template.
Only the Firewall Template is available because you have not created other templates yet.

5) Click **OK**.

6) Configure the Access and NAT rules as required for your environment.
To add a rule, right-click the green row, then select **Rule** > **Add Rule**. Add the matching criteria and the action to be taken for matching traffic. For more information, see the *Forcepoint Next Generation Firewall Product Guide*.

7) Click **Save and Install** to save the policy and transfer the changes to the NGFW Engine.

8) Select one or more NGFW Engines, then click **Add**.

9) Leave **Validate Policy Before Upload** selected to validate the rules in the policy.
Issues found in the policy are displayed in the tab that shows the progress of the policy installation.

10) Click **OK**.

Install a predefined policy on IPS engines and Layer 2 Firewalls

To be able to inspect traffic, the NGFW Engine must have a policy installed. Installing a predefined policy provides an easy way to begin using the system. You can then fine-tune the policy as needed.

Default Policy elements for IPS engines and Layer 2 Firewalls

Element type	Default element name	Description
IPS Template Policy	High-Security IPS Template	IPS Template Policy that uses Inspection rules from the High-Security Inspection Template. A Template Policy containing the predefined Access rules necessary for the IPS engine to communicate with the SMC and some external components. The High-Security IPS Template Policy provides an easy starting point for determining what kinds of rules your system needs.
	Medium-Security IPS Template	IPS Template Policy that uses Inspection rules from the Medium-Security Inspection Policy.
IPS Policy	Customized High-Security Inspection IPS Policy	Example of a customized IPS Policy that uses Inspection rules from the Customized High-Security Inspection Template. Used in testing Forcepoint NGFW in the IPS role at ICSA Labs and NSS Labs.
	Default IPS Policy	Basic IPS Policy that uses Inspection rules from the High-Security Inspection Template. Can be used as a starting point for creating a customized IPS Policy. The Default IPS Policy does not add any rules to the rules defined in the IPS Template. It allows you to install the predefined rules in the IPS Template on the IPS engine right after installation. (Template Policies cannot be installed on the NGFW Engine.)
Layer 2 Firewall Template Policy	Layer 2 Firewall Template	A Template Policy that contains the predefined Access rules necessary for the Layer 2 Firewall to communicate with the SMC and some external components. The Layer 2 Firewall Template uses Inspection rules from the No Inspection Policy. The rules in the No Inspection Policy do not enforce inspection.
	Layer 2 Firewall Inspection Template	A Template Policy that is based on the Layer 2 Firewall Template. The Layer 2 Firewall Inspection Template uses Inspection rules from the High-Security Inspection Template. The Layer 2 Firewall Inspection Template enables deep inspection for all traffic.

Element type	Default element name	Description
Inspection Policy	No Inspection Policy	Suitable for Firewall deployments, in which only packet filtering is needed. Disables deep packet inspection.
	Medium-Security Inspection Template	For Firewalls, Layer 2 Firewalls, inline IPS deployments in asymmetrically routed networks, and IPS deployments in IDS mode. Terminates reliably identified attacks and logs Situations that have some degree of inaccuracy. Low risk of false positives.
	High-Security Inspection Template	For Firewall, Layer 2 Firewall, and inline IPS use. Extended inspection coverage and evasion protection. Not for asymmetrically routed networks. Terminates reliably identified attacks, and Situations that have some inaccuracy. Moderate false positive risk.
	Customized High-Security Inspection Policy	This policy is an example of a highly customized Inspection Policy for network environments in which unconditional inspection coverage and evasion protection are required. The risk of false positives is high in production use.

The default policy elements might change when you import and activate a dynamic update package. You cannot modify any of the default policy elements, but you can make your own policies based on a copy of a default policy. For more information, see the *Forcepoint Next Generation Firewall Product Guide*.

Steps

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

1) Select **Configuration**.

2) Browse to **Policies** > **IPS Policies** or **Policies** > **Layer 2 Firewall Policies**.

3) Right-click a predefined policy, then select **Install Policy**.

4) Select one or more NGFW Engines, then click **Add**.

5) Click **OK**.
   A new tab opens to show the progress of the policy installation.

6) Check that the policy installation is successful.

Part IV
Maintenance

Contents

To maximize the benefit of Forcepoint NGFW, upgrade the SMC and Forcepoint NGFW regularly.

Chapter 12

Upgrading licenses

Contents

You must upgrade licenses if you upgrade the SMC, the SMC Appliance, or the NGFW Engines to a new major release.

Getting started with upgrading licenses

When you installed the SMC, the SMC Appliance, or the NGFW Engines for the first time, you installed licenses that work with all versions up to that particular version. Each license indicates the highest version for which the license is valid, but the license is also valid for all lower software versions.

A change in the first two digits of the version number indicates a major release (for example, from 1.2.3 to 1.3.0, or from 1.2.3 to 2.0.0). If only the last number changes, the existing license is also valid for the higher software version.

You can view and download your current licenses online at https://stonesoftlicenses.forcepoint.com. You can also upgrade the licenses.

Upgrade licenses manually

If you have not enabled automatic license upgrades, upgrade licenses manually through the Management Client.

Licenses are valid for any older software versions in addition to the version indicated on the license. You can upgrade the licenses at any time without affecting the system's operation.

Steps

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

1) Select **Configuration**, then browse to **Administration**.

2) Select **Licenses**, then browse to the type of licenses that you want to upgrade.

3) Select the license that you want to upgrade.
   Details about the selected license open in the **Info** pane.

4) In the **Info** pane, copy the license information to the clipboard in one of the following ways:

- From the **Proof of License** field, copy the POL code.
- From the **Proof of Serial** field, copy the POS code.

5) Go to https://stonesoftlicenses.forcepoint.com.

6) In the **License Identification** field, paste the POL or POS code, then click **Submit**.

7) Under the license information, click **Update**.

8) Enter any information needed for the upgrade request, then select the license files to update.

9) To send the license request, click **Submit**.
A confirmation page opens, showing the details of your request. The licenses are available for download on the license page.

Install licenses

After you have upgraded the licenses, install the license in the Management Client.

Steps

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

1) In the Management Client, select **Menu** > **System Tools** > **Install Licenses**.

2) Select the license files and click **Install**.

3) Select **Configuration**, then browse to **Administration**.

4) Browse to **Licenses** > **All Licenses**.

5) Check that the licenses have now been correctly upgraded to the new version.

Tip

When you only upgrade the software version in the license, old licenses are automatically replaced.

Check NGFW Engine licenses

After installing the upgraded NGFW Engine licenses, check the license information.

When you upgrade licenses, the old licenses are automatically replaced with the new licenses.

Steps

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

1) Select **Configuration**, then browse to **Administration**.

2) Browse to **Licenses** > **NGFW Engines**, **Licenses** > **Firewall**, or **Licenses** > **IPS**, depending on the type of licenses you have.
   The licenses and their status are displayed.

3) Verify that all NGFW Engines are correctly licensed.

4) If any NGFW Engines are not correctly licensed, you might need to upgrade or generate the licenses again.

Next steps

Continue the upgrade in one of the following ways:

- Upgrade the NGFW Engines remotely through the Management Server.
- Upgrade the NGFW Engines on the engine command line.

Chapter 13

SMC maintenance

Contents

When there is a new version available, upgrade the SMC before upgrading NGFW Engines.

Note

For information about SMC Appliance maintenance, see the SMC maintenance chapter.

Upgrading the SMC

You can upgrade SMC components without uninstalling the previous version.

Before upgrading, read the Release Notes.

It is important to upgrade the SMC components before upgrading NGFW Engines. An older SMC version might not be able to recognize the newer NGFW Engine version and can generate an invalid configuration for them. The Management Server can control several older versions of the NGFW Engine. See the release notes for version-specific compatibility information.

CAUTION

All SMC components (Management Server, Management Client, Log Server, and the optional Web Portal Server) must use the same software version to be able to work together. Plan ahead before upgrading the components. If you have multiple Management Servers and Log Servers, you must upgrade each server separately.

The NGFW Engines do not require a continuous connection to the SMC and they continue to operate normally during the SMC upgrade. The NGFW Engines temporarily store their logs locally if the Log Server is unavailable and then send them to the Log Server when it is available again.

For more detailed instructions, see the *Forcepoint Next Generation Firewall Product Guide*.

Configuration overview

Follow these general steps to upgrade the SMC.

1) Obtain the installation files and check the installation file integrity.

2) (If automatic license upgrades have been disabled) Upgrade the licenses.

3) Upgrade all components that work as parts of the same SMC.

4) (Multiple Management Servers only) Synchronize the management database between the Management Servers.

5) Upgrade the Management Clients that are installed locally on workstations.
If you are using the Management Client in a web browser through SMC Web Access, there is no need to upgrade.

Related concepts
Getting started with upgrading licenses on page 207

Related tasks
Upgrade SMC servers on page 212

Upgrade SMC servers

You can upgrade SMC servers without uninstalling the previous version. A change in the Management platform, such as a new operating system or different hardware, requires reinstalling the SMC.

CAUTION

All SMC components (Management Server, Management Client, Log Server, and the optional Web Portal Server) must use the same SMC software version to work together. If you have multiple Management Servers or Log Servers, you must upgrade each server separately.

The same installer works with all SMC components, including locally-installed Management Clients.

If you have multiple Management Servers or Log Servers, you can upgrade them in any order. Management Servers are automatically isolated from database replication during the upgrade. There is no need to explicitly isolate the Management Servers before upgrading.

If you are upgrading from a very old version of the SMC, you might have to upgrade to an intermediate version first before upgrading to the latest version. See the Release Notes.

Steps

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

1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.

2) Start the Installation Wizard from a .zip file or the Installation DVD.
Decompress the .zip file.
   - On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
   - On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

   If the DVD is not automatically mounted in Linux, use the following command:

   ```
   mount /dev/cdrom /mnt/cdrom
   ```

3) Select the language for the installation, then click **OK**.
The language that you select is also set as the default language of the Management Client.

4) Read the information on the **Introduction** page, then click **Next**.

Tip

Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.

5) Select **I accept the terms of the License Agreement**, then click **Next**.

6) To accept the installation directory that was automatically detected, click **Next**.
The Installation Wizard displays the components to be upgraded.

7) (Management Server only, optional) To save a copy of the current installation that you can revert to after the upgrade, select **Save Current Installation**, then click **Next**.

8) (Management Server only) Select whether to back up the server, then click **Next**.
- To create a backup that can be used and viewed without a password, select **Yes**.
- To create a password-protected backup, select **Yes, encrypt the backup**. You are prompted for the password as you confirm the selection.
- If you already have a recent backup of the Management Server, select **No**.

9) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.

10) (Optional) When the upgrade is complete, click the links in the notification to view the reports of changes the installer has made.
The report opens in your web browser.

11) When the installation has completed, click **Done**.

Next steps

1) Upgrade any SMC components that run on other computers (for example, additional Management Servers or Log Servers).

2) (Multiple Management Servers only) Synchronize the management database between the Management Servers.

Synchronize databases between the active Management Server and additional Management Servers

You must synchronize the configuration information manually through the Management Client after upgrading the Management Servers or after restoring a backup.

Before you begin

There must be a route between the Management Client and the Management Servers. If there is no route between the Management Client and the Management Servers, you cannot send a command through the SMC HA Administration dialog box.

Manual management database synchronization is primarily meant for resynchronizing the databases after upgrading the SMC. We do not recommend using manual database synchronization unless you have a specific need to do so.

Steps

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

1) Connect to the active Management Server using the Management Client.

2) Select **Menu** > **System Tools** > **SMC Servers HA Administration**.

3) If the Management Client is in a different network than the additional Management Server, select the **Location** from which to send the command.

4) For each additional Management Server that you want to synchronize:

   a) Right-click the Management Server, then select **Replication** > **Full Database Replication**.

   b) When prompted to confirm the replication, click **Yes**.
   All existing configurations on the additional Management Server are overwritten.

   c) Click **OK** to acknowledge the completion of the synchronization, then wait for the Management Server to restart.

Result

After the Management Server has restarted, its Replication Status is updated in the **SMC HA Administration** dialog box. Click **Close** to close the **SMC HA Administration** dialog box.

Uninstall the SMC

Usually, it is not necessary to uninstall the SMC, but you can do so if needed.

Note

If you have several SMC components installed on the same computer, you cannot uninstall the SMC components one by one.

By default, the SMC is installed in the following directories:

- Windows — `C:\Program Files\Forcepoint\SMC`
- Linux — `/usr/local/forcepoint/smc`

There is a .stonegate directory in each user's home directory in the operating system, which contains the Management Client configuration files. These files are not automatically deleted. You can delete them manually after the uninstallation.

The sgadmin account is deleted during the uninstallation of the SMC.

Tip

Back up the Management Server and the Log Server to an external system before uninstalling the SMC if you want to preserve the stored data.

Uninstall the SMC in Windows

Use this process to uninstall the SMC in a Windows environment.

Steps

1) Open the list of installed programs through the Windows Control Panel, right-click **Forcepoint NGFW Security Management Center**, then select **Uninstall/Change**.
   You can also run the script `<installation directory>\uninstall\uninstall.bat`

2) When the uninstaller opens, click **Uninstall**.

Result

All SMC components are uninstalled.

Uninstall the SMC in Linux

Use this process to uninstall the SMC in a Linux environment.

You can uninstall the SMC in graphical mode or in non-graphical mode.

Steps

1) Stop the Security Management Center components on the computer.

2) Run the uninstaller script.
   - To uninstall in graphical mode, run the script `<installation directory>/uninstall/uninstall.sh`.
   - To uninstall in non-graphical mode, run the script the script `<installation directory>/uninstall/uninstall.sh -nodisplay`.

3) (Graphical mode only) When the uninstaller starts, click **Uninstall**.

Result

All SMC components are uninstalled.

Chapter 14

SMC Appliance maintenance

Contents

The SMC Appliance has a specific patching process that keeps the SMC software, operating system, and appliance firmware up-to-date.

Getting started with SMC Appliance maintenance

SMC Appliance patches can include improvements, enhancements, and upgrades for the SMC software, the operating system, and the appliance firmware.

The SMC Appliance patch (SAP) format is specific to the SMC Appliance. The SAP numbering is appended to the version number. Patch digests are calculated using an SHA-512 hash and signed with an ECDSA key.

There are two kinds of SMC Appliance patches:

- Hotfix patches include improvements and enhancements for the current SMC Appliance version.
  Hotfix patch files use the letter P as a separator between the version number and the patch number. Example: 6.9.1P01
- Upgrade patches upgrade the SMC Appliance to a new version.
  Upgrade patch files use the letter U as a separator between the version number and the patch number. Example: 6.9.1U01

When you install a patch, a configuration backup and a file system snapshot are automatically created for the SMC Appliance. The backup and snapshot allow you to roll back the SMC Appliance to its previous configuration if needed. If the patch activation fails, the appliance reverts to the snapshot automatically. The file system of the SMC Appliance has two partitions: an active partition and an alternative partition. Some patches update the alternative partition. You can toggle between the partitions to roll back the SMC Appliance upgrade.

Note

SMC Appliance patches apply only to the SMC Appliance hardware or to SMC Appliance software installed on a virtualization platform. SMC components installed on third-party platforms do not offer a patching and rollback feature that includes the SMC software, the operating system, and the appliance firmware.

You can patch and upgrade the SMC Appliance remotely using the Management Client or using the appliance maintenance and bug remediation (AMBR) patching utility on the command line.

Configuration overview

1) Check for new SMC Appliance patches.
   There is no automatic notification when new SMC Appliance patches are available. We recommend checking for new SMC Appliance patches once a month.

2) Obtain the patch files.
   - You can use the Management Client or the AMBR utility to automatically download patch files directly into the Management Client or onto the SMC Appliance.
   - In environments without Internet connectivity, you must manually download patch files, then import them into the Management Client or transfer them to the SMC Appliance.

3) (If automatic license upgrades have been disabled) Upgrade the licenses.

4) Upgrade the Management Clients that are installed locally on workstations.
   If you are using the Management Client in a web browser through SMC Web Access, there is no need to upgrade.

Related concepts
Getting started with upgrading licenses on page 207

Patching and upgrading the SMC Appliance

To introduce improvements and enhancements for the current SMC Appliance version, install a hotfix patch. To upgrade the SMC Appliance, install an SMC Appliance upgrade patch.

Before upgrading, read the Release Notes.

It is important to upgrade the SMC Appliance before upgrading the engines. An old SMC version might not be able to recognize the new version engines and can generate an invalid configuration for them. The Management Server can control several older versions of engines. See the release notes for version-specific compatibility information.

Patch or upgrade the SMC Appliance in the Management Client

You can use the Management Client to patch or upgrade the SMC Appliance. In some certified environments, you must use the Management Client to install SMC Appliance patches.

Before you begin

In environments without Internet connectivity, you must download the SMC Appliance patch file from https://update.stonesoft.com/download/appliance/patches/, then transfer the file to a location that is accessible from the Management Client.

Installing some SMC Appliance patches might restart the SMC Appliance. The Restart Required column in the Management Client indicates whether the appliance must restart as part of the installation. You can use the Management Client to install SMC Appliance patches regardless of whether the installation requires restarting the SMC Appliance.

Steps

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

1) Select **Configuration**, then browse to **Administration**.

2) Browse to **SMC Appliance Patches**.

3) Download or import SMC Appliance patches.
   - To download an individual patch, right-click a patch for which the **State** column shows Available, then select **Download SMC Appliance Patch**.
   - To automatically download all available SMC Appliance patches, right-click **SMC Appliance Patches**, then select **Download SMC Appliance Patches**.
   - To import SMC Appliance patches that you manually downloaded, right-click **SMC Appliance Patches**, select **Import SMC Appliance Patches**, browse to the SMC Appliance patch file, then click **Import**.

4) Install a hotfix patch or an upgrade patch.
   - To patch the current SMC Appliance version, right-click a hotfix patch file, then select **Activate**.
   - To upgrade the SMC Appliance to a new version, right-click an upgrade patch file, then select **Activate**.

Result

The SMC Appliance patch is installed on the SMC Appliance.

If you installed an SMC Appliance upgrade patch, the installation process restarts the appliance and installs the patch. When the upgrade is finished, the appliance restarts again.

Patch or upgrade the SMC Appliance on the command line

You can use the appliance maintenance and bug remediation (AMBR) patching utility to patch or upgrade the SMC Appliance on the command line.

Before you begin

In environments without Internet connectivity, you must download the SMC Appliance patch file from https://update.stonesoft.com/download/appliance/patches/, then transfer the files to the SMC Appliance.

If you do not have physical access to the SMC Appliance, use SSH to access the SMC Appliance remotely.

Note

In FIPS mode, SSH access to the SMC Appliance command line is not supported.

You must have SMC Appliance Superuser permissions to log on to the SMC Appliance command line. Administrators with unrestricted permissions (superusers) are allowed to log on to the SMC Appliance command line only if there are no administrators with Console Superuser permissions.

Use sudo if you need elevated privileges. For a list of available sudo commands, enter the following command:

```
sudo -l
```

Steps

1) From the command line, log on to the SMC Appliance.

2) To update the list of available remote patches from the download server, enter the following command:

```
sudo ambr-query -u
```

3) To show all local and remote patches, enter the following command:

```
sudo ambr-query -a
```

4) To automatically download a patch, or to load a patch that you manually downloaded, enter the following command:

```
sudo ambr-load <patch>
```

Note

If you manually downloaded the patch and transferred it to the SMC Appliance, append the command with the `-f` option and specify the full path to the patch file.

Example:

```
sudo ambr-load –f /var/tmp/6.9.0P001.sap
```

5) To activate the patch, enter the following command:

```
sudo ambr-install <patch>
```

Result

The SMC Appliance patch is installed on the SMC Appliance.

If you installed an SMC Appliance upgrade patch, the installation process restarts the appliance and installs the patch. When the upgrade is finished, the appliance restarts again.

Related reference
Security Management Center commands on page 243

Unload SMC Appliance patches on the command line

When you load patches, they are copied to the patch storage on the SMC Appliance. Use the unload command to remove patches that have been loaded but not installed from the patch storage on the SMC Appliance.

Note

To revert changes made by a patch that has been installed, roll back the SMC Appliance to the previous version.

Steps

1) From the command line, log on to the SMC Appliance.

2) To unload the patch, enter the following command:

```
sudo ambr-unload <patch>
```

Result

The patch is removed from the patch storage on the SMC Appliance. To verify that it has been removed, enter the following command:

```
ambr-query
```

Note

Patch files that you manually transferred to the SMC Appliance are removed from the patch storage, but are not deleted from the file system of the SMC Appliance. You must manually delete these patch files.

Roll back the SMC Appliance to the previous version on the command line

To revert changes made by a patch that has been installed, you can roll back the SMC Appliance to the previous configuration if needed.

Note

When you roll back the SMC Appliance, configuration changes made after the current version was installed are lost. We recommend rolling back as a recovery option only for a short time after an upgrade.

Steps

1) From the command line, log on to the SMC Appliance.

2) Enter the following command:

```
sudo smca-system toggle
```

3) Restart the SMC Appliance.

Result

When the SMC Appliance restarts, the previous SMC Appliance configuration is in use.

Chapter 15

Upgrading NGFW Engines

Contents

When a new version of Forcepoint Next Generation Firewall introduces features that you want to use, upgrade the Forcepoint NGFW engines.

How engine upgrades work

You can remotely upgrade engines using the Management Client or locally on the engine command line.

The upgrade package is imported to the Management Server manually or automatically. Upgrade package digests are calculated using an SHA-512 hash and signed with an ECDSA key.

Before the import, the Management Server verifies the digital signature of the upgrade package using a valid Trusted Update Certificate. The signature must be valid for the import to succeed. Verification might fail for the following reasons:

- The SMC version is out of date. Upgrade the SMC before upgrading the engines.
- A signature is invalid or missing in the upgrade files. Obtain an official upgrade package.

After the upgrade package has been imported, you can apply it to selected engines through the Management Client. Before the upgrade is installed on the engines, the Management Server again verifies the digital signature of the upgrade package. The engines also verify the digital signature of the upgrade package before the upgrade is installed.

The engines have two alternative partitions for the software. When you install a new software version, it is installed on the inactive partition and the current version is preserved. This configuration allows rollback to the previous version in case there are problems with the upgrade. If the engine is not able to return to operation after the upgrade, it automatically changes back to the previous software version at the next restart. You can also change the active partition manually.

You can upload and activate the new software separately. For example, you can upload the upgrade during office hours but activate it during a service window.

The currently installed working configuration (routing, policies) is stored separately and is not changed in an upgrade or a rollback. Although parts of the configuration can be version-specific (for example, if system communications ports are changed), the new software version can use the existing configuration. Possible version-specific adjustments are made when you refresh the policy after the upgrade.

Lifecycle models

There are two types of Forcepoint Next Generation Firewall releases:

- Long-Term Support (LTS) — Long-Term Support versions are major versions of Forcepoint Next Generation Firewall that are maintained for at least two years from the release date.
- Feature Stream (FS) — Feature Stream versions are major versions of Forcepoint Next Generation Firewall that introduce new features and enhancements. Support for Feature Stream versions is discontinued when a new major version of Forcepoint Next Generation Firewall is available.

We recommend using the most recent Long-Term Support version of Forcepoint Next Generation Firewall if you do not need any features from a later Feature Stream version.

For more information about the Forcepoint Next Generation Firewall lifecycle policy, see Knowledge Base article 10192.

Limitations

It is not possible to upgrade between a 32-bit version and a 64-bit version of the software. If you are running the software on third-party hardware, you can reinstall the software using the other version. In clusters, 32-bit and 64-bit nodes cannot be online simultaneously. Appliances support only the software architecture version that they are preinstalled with.

You cannot upgrade Virtual NGFW Engines directly. To upgrade Virtual NGFW Engines, you must upgrade the Master NGFW Engine that hosts the Virtual NGFW Engines.

What do I need to know before I begin?

The SMC must be up to date before you upgrade the engines. An old SMC version might not be able to recognize the new version engines and can generate an invalid configuration for them. The Management Server can control several older versions of engines. See the Release Notes for version-specific compatibility information.

During a cluster upgrade, it is possible to have the upgraded nodes online and operational side by side with the older version nodes. This way, you can upgrade the nodes one by one while the other nodes handle the traffic. However, you must upgrade all nodes to the same version as soon as possible, as prolonged use with mismatched versions is not supported.

The current engine version is displayed on the **General** tab in the **Info** pane when you select the engine. If the **Info** pane is not shown, select ☰ **Menu** > **View** > **Panels** > **Info**.

Beginning from version 5.9, all Forcepoint Next Generation Firewall licenses include the anti-malware feature by default.

Configuration overview

Follow these general steps to upgrade engines:

1) (Manual download of engine upgrade files) Prepare the installation files.

2) (Manual license updates) Update the licenses.

3) Upgrade the engines.

Obtain NGFW Engine upgrade files

If the Management Server is not set up to download engine upgrades automatically or if you want to upgrade engines locally, download the installation files manually.

Check the installation file integrity using the MD5 or SHA-1 file checksums. Windows does not have MD5 or SHA-1 checksum programs by default, but there are several third-party programs available.

Steps

1) Go to https://support.forcepoint.com.

2) Enter your license code or log on using an existing user account.

3) Select **Downloads**.

4) Under **Network Security**, click the version of the Forcepoint NGFW software that you want to download, then select the type of installation file to download.
   - The .zip file is used in the remote upgrade on all supported platforms. It can also be used for a local upgrade from a USB drive or a non-bootable DVD.
   - The .iso file allows you to create a bootable installation DVD for a local upgrade on platforms that have an optical drive.

5) On your local computer, change to the directory that contains the files to be checked.

6) (Linux only) Generate a checksum of the file using one of the following commands, where `filename` is the name of the installation file:
   - `sha1sum filename`
   - `sha256sum filename`
   - `sha512sum filename`

   For Windows, see the documentation for the third-party checksum program.

   Example:

   ```
   $ sha1sum sg_engine_1.0.0.1000.iso
   869aecd7dc39321aa2e0cfaf7fafdb8f sg_engine_1.0.0.1000.iso
   ```

7) Compare the displayed output to the checksum on the website.

   CAUTION

   Do not use files that have invalid checksums. If downloading the files again does not help, contact Forcepoint support to resolve the issue.

Next steps

Prepare NGFW Engine upgrade files.

Related tasks
Upgrade NGFW Engines remotely on page 227
Upgrade engines locally on page 229

Prepare NGFW Engine upgrade files

Prepare the NGFW Engine upgrade files depending on the type of files you downloaded and how you plan to upgrade.

Steps

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

1) To prepare a downloaded .zip file for a remote upgrade, follow these steps.
   a) Log on to the Management Client and select **Menu** > **File** > **Import** > **Import Engine Upgrades**.
   b) Select the engine upgrade (**sg_engine_version_platform.zip**) file and click **Import**.

   Note

   The Management Server verifies the digital signature of the .zip file before importing it. The signature must be valid for the import to succeed. If the verification fails, an error message is shown. Verification failure can result from an out-of-date SMC version or an invalid or missing signature.

   The status bar at the bottom of the Management Client window shows the progress of the import.

2) To prepare a downloaded .zip file for a local upgrade, copy the file to the root directory of a USB drive or a DVD.

3) To prepare a downloaded .iso file for a local upgrade, create the installation DVD for the engines with a DVD burning application that can correctly read and burn the DVD structure stored in the .iso images.
   If the end result is a DVD file with the original .iso file on it, the DVD cannot be used for installation.

Next steps

Continue in one of the following ways:

- If your license does not support the version that you are upgrading to, upgrade or generate licenses.
- Upgrade the engines remotely through the Management Server.
- Upgrade the engine locally at the engine site.

Upgrade NGFW Engines remotely

The Management Server can remotely upgrade NGFW Engine components that it manages.

Before you begin

Read the Release Notes for the new version, especially the required SMC version and any other version-specific upgrade issues that might be listed. To access the release notes, select **Configuration**, then browse to **Administration** > **Other Elements** > **Engine Upgrades**. Select the type of NGFW Engine you are upgrading. A link to the release notes is included in the upgrade file's information. If the Management Server has no Internet connectivity, you can find the release notes at https://support.forcepoint.com/Documentation.

CAUTION

If McAfee Endpoint Intelligence Agent (McAfee EIA) is configured on the NGFW Engine when you upgrade to version 6.3 or later, the NGFW Engine node is returned to the initial configuration state and stops processing traffic. You must remove the McAfee Endpoint Intelligence Agent (McAfee EIA) configuration and refresh the policy before you upgrade to version 6.3 or later. For more information, see Knowledge Base article 14093.

You can upgrade several NGFW Engines of the same type in the same operation. However, we recommend that you upgrade clusters one node at a time and wait until an upgraded node is back online before you upgrade the other nodes. Clusters operate normally throughout the upgrade when the upgrade is done in stages. However, it is recommended to upgrade all nodes in the cluster to the same version as soon as possible. Prolonged use with mismatched versions is not supported. It is not possible to have 32-bit and 64-bit NGFW Engines online in the cluster at the same time.

Steps

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

1) Select **Home**.
2) Browse to **Engines**, then expand the nodes of the NGFW Engine that you want to upgrade.
3) Right-click the node that you want to upgrade, then select **Commands** > **Go Offline**.
4) (Optional) Enter an **Audit Comment** to be shown in the audit log entry that is generated when you send the command to the NGFW Engine.
5) When prompted to confirm that you want to set the node offline, click **Yes**.
   The node goes offline shortly.

6) When the node is offline, right-click the node, then select **Upgrade Software** or **Configuration** > **Upgrade Software** depending on your selection.

Note

You cannot upgrade Virtual NGFW Engines directly. To upgrade Virtual NGFW Engines, you must upgrade the Master NGFW Engine that hosts the Virtual NGFW Engines.

7) From the **Operation** drop-down list, select the type of operation that you want to perform:

- Select **Remote Upgrade (transfer + activate)** to install the new software and reboot the node with the new version of the software.
- Select **Remote Upgrade (transfer)** to install the new software on the node without an immediate reboot and activation. The node continues to operate with the currently installed version until you choose to activate the new version.
- Select **Remote Upgrade (activate)** to reboot the node and activate the new version of the software that was installed earlier.

CAUTION

To avoid an outage, do not activate the new configuration simultaneously on all nodes of a cluster. Activate the new configuration one node at a time, and proceed to the next node only after the previous node is back online.

8) If necessary, add or remove NGFW Engines in the **Target** list.

All NGFW Engines in the same Upgrade Task must be of the same type.

9) Click **Select** next to the **Engine Upgrade** field, select the upgrade file, then click **OK**.

If you choose to activate the new configuration, you are prompted to acknowledge a warning that the node will be rebooted. A new tab opens showing the progress of the upgrade. The time the upgrade takes varies depending on the performance of your system and the network environment. The NGFW Engine is automatically rebooted and brought back online.

The upgrade overwrites the inactive partition and then changes the active partition. To undo the upgrade, use the `sg-toggle-active` command or the NGFW Engine's boot menu to change back to the previous software version on the other partition. This change can also happen automatically at the next reboot if the NGFW Engine is not able to successfully return to operation when it boots up after the upgrade.

Note

The Management Server verifies the digital signature of the upgrade package before installing it. The signature must be valid for the upgrade to succeed. If the verification fails, an error message is shown. Verification failure can result from an out-of-date SMC version or an invalid or missing signature.

Upgrade engines locally

You can upgrade the engines on the engine command line.

Before you begin

Upgrading locally requires a physical connection to the engine using a monitor and keyboard or a serial cable.

CAUTION

If McAfee Endpoint Intelligence Agent (McAfee EIA) is configured on the NGFW Engine when you upgrade to version 6.3 or later, the NGFW Engine node is returned to the initial configuration state and stops processing traffic. You must remove the McAfee Endpoint Intelligence Agent (McAfee EIA) configuration and refresh the policy before you upgrade to version 6.3 or later. For more information, see Knowledge Base article 14093.

During a Firewall Cluster or Master NGFW Engine cluster upgrade, the upgraded nodes can be online and operational side by side with the older version nodes. However, you must upgrade all nodes to the same version as soon as possible, as prolonged use with mismatched versions is not supported.

There are two ways to upgrade engines locally:

- If the hardware has a DVD drive (a USB DVD drive can be used) and you have an installation DVD, you can upgrade from an installation DVD.
- You can upgrade from a .zip file on a USB drive or on a DVD.

Upgrade from an installation DVD

You can upgrade the engines to the latest version from a DVD that was shipped to you, or from a DVD that you have created from an .iso image that you downloaded from the Forcepoint website.

Steps

1) Log on to the node as root with the password you set for the engine (you can set the password through the Management Client).

2) Insert the DVD into the engine's DVD drive.

3) Restart the node from the DVD with the command `reboot` (recommended) or by cycling the power (if you cannot log on).
   You are promoted to select the upgrade type.

4) Enter `1` to upgrade the existing installation and press **Enter** to continue.
   The upgrade process starts.

5) When the process is finished, eject the DVD and press **Enter** to restart.

6) If the command-line version of the NGFW Configuration Wizard opens, configure the engine in the same way as after the first installation.
   You can also use the web browser version of the NGFW Configuration Wizard.

7) When the upgrade is finished, right-click the node in the Management Client and select **Commands** > **Go Online**.
   A confirmation dialog box opens.

8) (Optional) Enter an **Audit Comment** to be shown in the audit log entry that is generated when you send the command to the engine.

9) Click **Yes**.

Note

If you are upgrading a cluster, start the upgrade on the next node only when the upgraded node is back online.

Related tasks
Using the NGFW Configuration Wizard on page 188

Upgrade from a .zip file

You can use a .zip file to upgrade the engine software locally on the engine command line.

Steps

1) Log on to the node as root with the password set for the engine (you can set the password through the Management Client).

2) Insert the USB drive or the DVD.

3) Run the command `sg-reconfigure`.
   The NGFW Configuration Wizard opens.

4) Select **Upgrade** and press **Enter**.

5) Select the source media where the upgrade file is located.

6) Select **OK**.
   The software is upgraded.

Note

The NGFW Engine verifies the digital signature of the upgrade package before installing it. The verification can take several minutes. The signature must be valid for the upgrade to succeed. If the verification fails, an error message is shown. Verification failure can result from an out-of-date Forcepoint NGFW software version or an invalid or missing signature.

7) When prompted, press **Enter**.
The engine restarts with the new version.

Appendices

Contents

Appendix A

Default communication ports

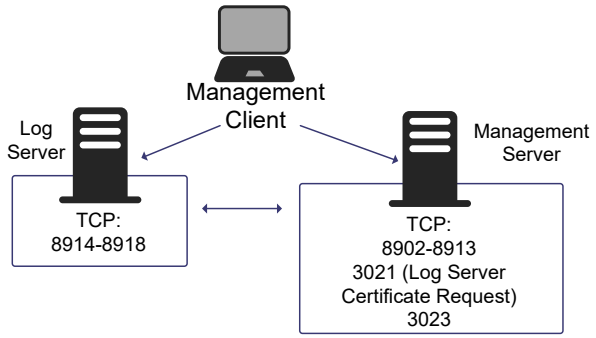
Contents

There are default ports used in connections between SMC components and default ports that SMC components use with external components.

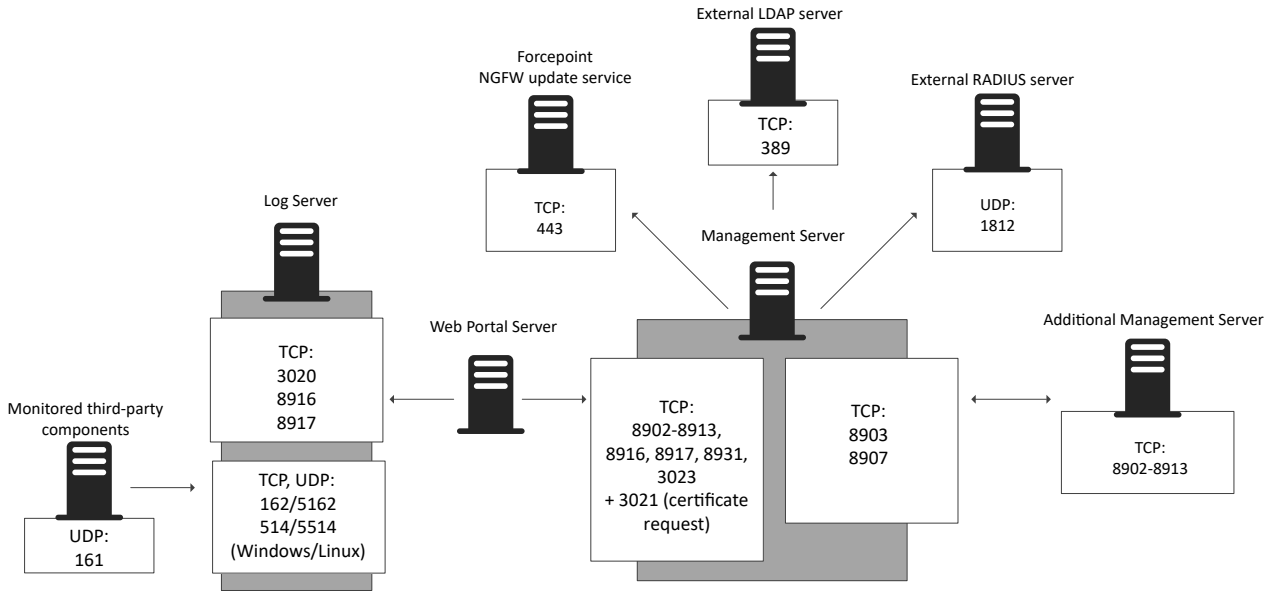
Security Management Center ports

The most important default ports used in communications to and from SMC components are presented in the following illustrations.

Destination ports for basic communications within the SMC



Default destination ports for optional SMC components and features



This table lists the default ports SMC uses internally and with external components. Many of these ports can be changed. The names of corresponding default Service elements are also included for your reference.

SMC default ports

Listening host	Port/protocol	Contacting hosts	Service description	Service element name
Additional Management Servers	8902- 8913/TCP	Management Server	Database replication (push) to the additional Management Server.	SG Control
DNS server	53/UDP, 53/TCP	Management Client, Management Server, Log Server	DNS queries.	DNS (UDP)
LDAP server	389/TCP	Management Server	External LDAP queries for display/editing in the Management Client.	LDAP (TCP)
Log Server	162/UDP, 5162/UDP	Monitored third-party components	SNMPv1 trap reception from third-party components. Port 162 is used if installed on Windows, port 5162 if installed on Linux.	SNMP (UDP)
Log Server	514/TCP, 514/UDP, 5514/TCP, 5514/UDP	Monitored third-party components	Syslog reception from third-party components. Port 514 is used if installed on Windows, port 5514 if installed on Linux.	Syslog (UDP) [Partial match]
Log Server	2055/UDP	Monitored third-party components	NetFlow or IPFIX reception from third-party components. Port 2055 is used in both Windows and Linux.	NetFlow (UDP)

Listening host	Port/protocol	Contacting hosts	Service description	Service element name
Log Server	3020/TCP	Log Server, Web Portal Server, NGFW Engines	Alert sending from the Log Server and Web Portal Server. Log and alert messages; monitoring of blacklists, connections, status, and statistics from NGFW Engines.	SG Log
Log Server	8914-8918/TCP	Management Client	Log browsing.	SG Data Browsing
Log Server	8916-8917/TCP	Log Server, Web Portal Server	Database replication (push) to the Log Server; Log browsing on the Web Portal Server.	SG Data Browsing (Web Portal Server)
Management Server	3021/TCP	Log Server, Web Portal Server	System communications certificate request/renewal.	SG Log Initial Contact
Management Server	8902-8913/TCP	Management Client, Log Server, Web Portal Server	Monitoring and control connections.	SG Control
Management Server	3023/TCP	Additional Management Servers, Log Server, Web Portal Server	Log Server and Web Portal Server status monitoring. Status information from an additional Management Server to the active Management Server.	SG Status Monitoring
Management Server	8903, 8907/TCP	Additional Management Servers	Database replication (pull) to the additional Management Server.	SG Control
Management Server	8085/TCP	SMC Web Access clients	Communication for using SMC Web Access.	HTTPS
Monitored third-party components	161/UDP	Log Server	SNMP status probing to external IP addresses.	SNMP (UDP)
NTP server	123/TCP or UDP	SMC Appliance	Receiving NTP information.	NTP
RADIUS server	1812/UDP	Management Server	RADIUS authentication requests for administrator logon. The default ports can be edited in the properties of the RADIUS Server element.	RADIUS (Authentication)
Forcepoint NGFW update service	443/TCP	SMC servers	Update packages, engine upgrades, and licenses.	HTTPS
SMC Appliance	161/UDP	Third-party components	Requesting health and other information about the SMC Appliance.	SNMP
Update servers	443/TCP	SMC Appliance	Receiving appliance patches and updates.	HTTPS
SMC Appliance	22/TCP	Terminal clients	SSH connections to the command line of the SMC Appliance.  **Note** Do not use SSH in FIPS mode.	SSH

Listening host	Port/protocol	Contacting hosts	Service description	Service element name
Syslog server	514/UDP, 5514/UDP	Log Server	Log data forwarding to syslog servers. The default ports can be edited in the LogServerConfiguration.txt file.	Syslog (UDP) [Partial match]
Terminal Client Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	22/TCP	SMC Appliance	Contacting engines and moving SMC Appliance backups off the appliance. **Note** Do not use SSH in FIPS mode.	SSH
Third-party components	2055/UDP	Log Server	NetFlow or IPFIX forwarding to third-party components. Port 2055 is used in both Windows and Linux.	NetFlow (UDP)
Third-party components	162/UDP	SMC Appliance	Sending SNMP status probing to external devices.	SNMP
Third-party components	445/TCP	SMC Appliance	Moving SMC Appliance backups off the appliance. **Note** You cannot use CIFS in FIPS mode.	CIFS
Web Portal Server	8931/TCP	Log Server	Connections from the Log Server to the Web Portal Server	SG Web Portal Control
Web Portal Server	8083/TCP	SMC Web Access clients	Communication for using SMC Web Access.	HTTPS

Forcepoint NGFW Engine ports

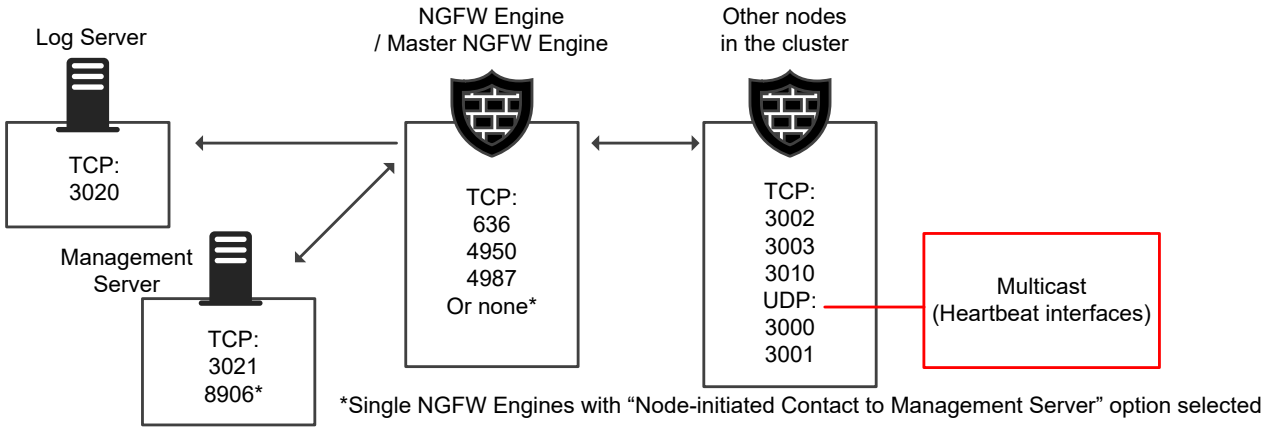
The most important default ports used in communications to and from NGFW Engines and Master NGFW Engines are presented in the following illustrations.

See the table for a complete list of default ports for the engines.

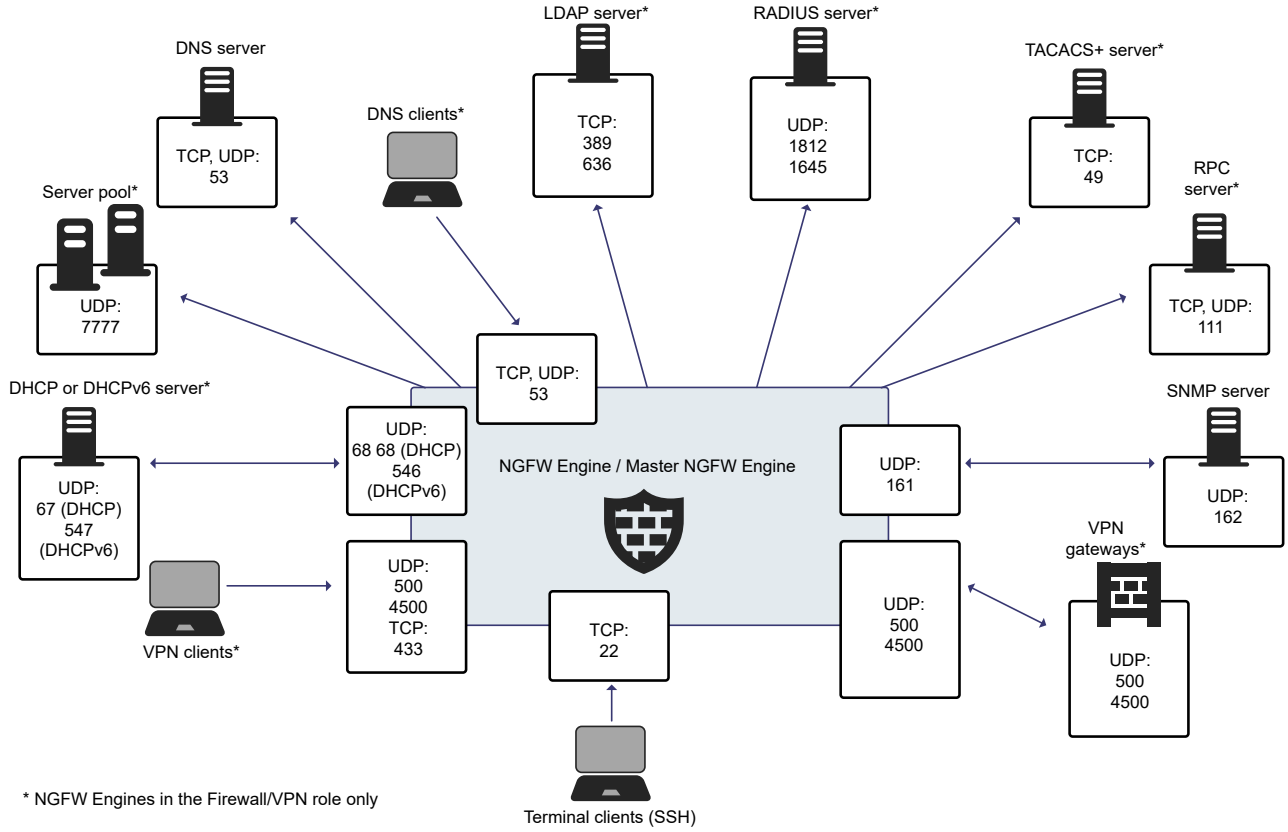
Note

Master NGFW Engines use the same default ports as clustered NGFW Engines. Virtual NGFW Engines do not communicate directly with other system components.

Destination ports for basic NGFW Engine communications



Default destination ports for NGFW Engine service communications



This table lists the default ports for NGFW Engines and Master NGFW Engines. Many of these ports can be changed. The names of corresponding default Service elements are also included for your reference.

NGFW Engine and Master NGFW Engine default ports

Listening host	Port/protocol	Contacting hosts	Service description	Service element name
Certificate Revocation List (CRL) server	80/TCP	Firewall	Online certificate status protocol (OCSP) queries and fetching CRLs.	HTTP

Listening host	Port/protocol	Contacting hosts	Service description	Service element name
DHCP server	67/UDP	Firewall	Relayed DHCP requests and requests from a firewall that uses dynamic IP address.	BOOTPS (UDP)
DHCPv6 server	547/UDP	Firewall	Requests from a firewall that uses dynamic IPv6 address.	N/A
External DNS server	53/UDP, 53/TCP	Firewall, Master NGFW Engine	DNS resolution and dynamic DNS updates.	DNS (TCP), DNS (UDP)
File reputation server	443/TCP	Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	GTI File Reputation Server	HTTPS
Firewall	67/UDP	Any	DHCP relay on firewall engine.	BOOTPS (UDP)
Firewall	68/UDP	DHCP server	Replies to DHCP requests.	BOOTPC (UDP)
Firewall	80/TCP	Clients that need to authenticate to the Firewall	Browser Based User Authentication	HTTP
Firewall	443/TCP	Clients that need to authenticate to the Firewall	Browser Based User Authentication	HTTPS
Firewall	443/TCP	VPN clients using SSL tunneling	VPN client SSL tunneling	TLS
Firewall	443/TCP	SSL Portal users	SSL VPN Portal	HTTPS
Firewall	546/UDP	DHCPv6 server	Replies to DHCPv6 requests.	N/A
Firewall, Master NGFW Engine	53/UDP, 53/TCP	Clients in the internal network	DNS relay	DNS (TCP), DNS (UDP)
Firewall, Master NGFW Engine	500/UDP	VPN clients, VPN gateways	VPN negotiations, VPN traffic.	ISAKMP (UDP)
Firewall, Master NGFW Engine	636/TCP	Management Server	Internal user database replication.	LDAPS (TCP)
Firewall, Master NGFW Engine	4500/UDP	VPN client, VPN gateways	VPN traffic using NAT-traversal.	NAT-T
Firewall Cluster Node, Master NGFW Engine cluster node	3000-3001/UDP, 3002–3003, 3010/TCP	Firewall Cluster Node, Master NGFW Engine cluster node	Heartbeat and state synchronization between clustered Firewalls.	SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync
Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	22/TCP	Terminal clients	SSH connections to the engine command line. **Note** Do not use SSH in FIPS mode.	SSH
Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	4950/TCP	Management Server	Remote upgrade.	SG Remote Upgrade

Listening host	Port/protocol	Contacting hosts	Service description	Service element name
Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	4987/TCP	Management Server	Management Server commands and policy upload.	SG Commands
Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	15000/TCP	Management Server, Log Server	Blacklist entries.	SG Blacklisting
Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	161/UDP	SNMP server	SNMP monitoring.	SNMP (UDP)
Firewall, Layer 2 Firewall, IPS	9111/TCP	Forcepoint Endpoint Context Agent (ECA) client	Endpoint information from the ECA client.	N/A
Forcepoint User ID Service server	5000/TCP	Firewall, Layer 2 Firewall, IPS	Information about user name and IP address mappings.	N/A
IPS Cluster Node	3000-3001/UDP, 3002–3003, 3010/TCP	IPS Cluster Node	Heartbeat and state synchronization between clustered IPS engines.	SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync
LDAP server	389/TCP	Firewall, Master NGFW Engine	External LDAP queries, including StartTLS connections.	LDAP (TCP)
Layer 2 Firewall Cluster Node	3000-3001/UDP, 3002–3003, 3010/TCP	Layer 2 Firewall Cluster Node	Heartbeat and state synchronization between clustered Layer 2 Firewalls.	SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync
Log Server	3020/TCP	Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	Log and alert messages; monitoring of blacklists, connections, status, and statistics.	SG Log
Malware signature server	80/TCP	Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	Malware signature update service.	HTTP
Management Server	3021/TCP	Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	System communications certificate request/renewal (initial contact).	SG Initial Contact
Management Server	8906/TCP	Firewall, Layer 2 Firewall, IPS	Management connection for engines with "Node-Initiated Contact to Management Server" selected.	SG Dynamic Control
RADIUS server	1812, 1645/UDP	Firewall, Master NGFW Engine	RADIUS authentication requests.	RADIUS (Authentication), RADIUS (Old)
RPC server	111/UDP, 111/TCP	Firewall, Master NGFW Engine	RPC number resolve.	SUNRPC (UDP), Sun RPC (TCP)
Server Pool Monitoring Agents	7777/UDP	Firewall, Master NGFW Engine	Polls to the servers' Server Pool Monitoring Agents for availability and load information.	SG Server Pool Monitoring

Listening host	Port/protocol	Contacting hosts	Service description	Service element name
SNMP server	162/UDP	Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	SNMP traps from the engine.	SNMP Trap (UDP)
TACACS+ server	49/TCP	Firewall, Master NGFW Engine	TACACS+ authentication requests.	TACACS (TCP)
ThreatSeeker Intelligence Cloud server	443/TCP	Firewall, Layer 2 Firewall, IPS, Master NGFW Engine	ThreatSeeker Intelligence Cloud URL categorization service.	HTTPS
VPN gateways	500, 4500/UDP	Firewall, Master NGFW Engine	VPN traffic. Ports 443/TCP (or custom port) can also be used, depending on encapsulation options.	ISAKMP (UDP)

Appendix B

Command line tools

Contents

There are command line tools for the SMC and the NGFW Engines.

Security Management Center commands

SMC commands include commands for the Management Server, Log Server, and Web Portal Server.

In Windows, the command line tools are *.bat script files. In Linux, the files are *.sh scripts. Commands are found in the following locations:

- For SMC installations on Linux or Windows, commands are found in the `<installation directory>/bin` directory.
- For the SMC Appliance, general SMC commands are found in the `/usr/local/forcepoint/smc/bin` directory.
- Commands that are specific to the SMC Appliance are found in the `/usr/bin` directory.

On the SMC Appliance, commands must be run with elevated permissions using sudo. A list of available sudo commands can be found by running `sudo -l` at the command line.

Note

Only administrators who have SMC Appliance Superuser administrator permissions can log on to the SMC Appliance command line.

Commands that require parameters must be run through the command line (cmd.exe in Windows). Commands that do not require parameters can alternatively be run through a graphical user interface, and can be added as shortcuts during installation.

CAUTION

`login` and `password` parameters are optional. Giving them as command-line parameters can pose a security vulnerability. Do not enter logon and password information unless explicitly prompted to do so by a command line tool.

Security Management Center commands

Command	Description

`ambr-crl`
(SMC Appliance only)
`[-a ADD|--add=ADD]`
`[-d DELETE|--delete=DELETE]`
`[-q|--query]`
`[-i IMPORT_CRL|--import=IMPORT_CRL]`
`[-v]`
`[-l <log file path>]`
`[-h|--help]`
	Fetches the certificate revocation lists (CRLs) for the CA certificates used by the appliance maintenance and bug remediation (AMBR) utilities.
	`-a ADD, --add=ADD` adds a CRL distribution point URL in the form of `http://<url>`.
	`-d DELETE, --delete=DELETE` deletes a CRL distribution point URL.
	`-q, --query` lists CRL distribution points.
	`-i IMPORT_CRL, --import=IMPORT_CRL` imports a CRL from a file.
	`-v` increases the verbosity of the command. You can repeat this command up to two times (`-vv` or `-v -v`) to further increase the verbosity.
	`-l <log file path>` specifies the path to a log file.
	`-h, --help` shows information about the command.

`ambr-decrypt` (SMC Appliance only)	Decrypts an ambr patch; not normally used by administrators. `ambr-install` automatically decrypts patches.

`ambr-install <patch>`
(SMC Appliance only)
`[-F|--force]`
`[-r|--skip-revocation]`
`[--no-backup]`
`[--no-snapshot]`
`[--no-prompt]`
`[-v]`
`[-l <log file path>]`
`[-h|--help]`
	Installs an ambr patch that has been loaded on the system.
	You can install multiple patches with a space between each patch name.
	`-F, --force` forces the reinstallation of the patch or patches.
	`-r, --skip-revocation` skips the certificate revocation checks.
	`--no-backup` does not create a configuration backup.
	`--no-snapshot` does not create a recovery snapshot.
	`--no-prompt` does not prompt before restarting.
	`-v` increases the verbosity of the command. You can repeat this command up to two times to further increase the verbosity.
	`-l <log file path>` specifies the path to a log file.
	`-h, --help` shows information about the command.

`ambr-load <patch>`
(SMC Appliance only)
`[-f IN_FILES|--file=IN_FILES]`
`[-r|--skip-revocation]`
`[-v]`
`[-l <log file path>]`
`[-h|--help]`
	Loads an ambr patch onto the system from either the patch server or from the local file system. A loaded patch means that the file is copied to the local file system, but not installed.
	You can load multiple patches with a space between each patch name.
	`-f IN_FILES, --file=IN_FILES` specifies the local file to load.
	`-r, --skip-revocation` skips the certificate revocation checks.
	`-v` increases the verbosity of the command. You can repeat this command up to two times to further increase the verbosity.
	`-l <log file path>` specifies the path to a log file.
	`-h, --help` shows information about the command.

Command	Description

`ambr-query`
(SMC Appliance only)
`[-c|--clean]`
`[-u|--update]`
`[-a|--all]`
`[-j|--json]`
`[-i INFO|--info=INFO <patch>]`
`[-L <log file path>]`
`[-v]`
`[-h|--help]`
	Shows patch information including:
	■ What is loaded or installed on the system
	■ A list of available updates from the patch server
	■ Detailed information about a specific patch
	`-u , --update` updates the remote patch list from a web server .
	`-c, --clean` cleans the remote patch cache.
	`-a, --all` shows all local and remote patches.
	`-j, --json` formats output as JSON.
	`-i INFO, --info=INFO <patch>` shows detailed information about the patch. You can get information about multiple patches in one command by separating the patch names with a space.
	`-v` increases the verbosity of the command. You can repeat this command up to two times to further increase the verbosity.
	`-L <log file path>` specifies the path to the file where log messages are written.
	`-h, --help` shows information about the command.

`ambr-unload <patch>`
(SMC Appliance only)
`[-a|--all]`
`[-v]`
`[-l <log file path>]`
`[-h|--help]`
	Unloads an ambr patch from the system. The command deletes the patch file if it has not been installed, but it does not uninstall the patch.
	You can unload multiple patches with a space between each patch name.
	`-a, --all` unloads all loaded patches.
	`-v` increases the verbosity of the command. You can repeat this command up to two times to further increase the verbosity.
	`-l <log file path>` specifies the path to a log file.
	`-h, --help` shows information about the command.

`ambr-verify` (SMC Appliance only)	Verifies the signature of a patch file; not normally used by administrators. `ambr-install` automatically verifies patches.
`cloudDiscoveryCLI` (Requires installation of the Cloud Discovery Tool)	Processes log data exported from the SMC to produce a summary report about cloud application usage. To use exported log data with the Cloud Discovery Tool, the data must be in Short CSV format.

Command	Description

`sgArchiveExport`
`[host=<Management Server Address[\Domain>]`
`[login=<login name>]`
`[pass=<password>]`
`[format=<exporter format: CSV or XML>]`
`i=<input files and/or directories>`
`[o=<output file name>]`
`[f=<filter file name>]`
`[e=<filter expression>]`
`[-h|-help|-?]`
`[-v]`
	Shows and exports logs from archive. Supports CEF, LEEF, and ESM formats in addition to CSV and XML.
	This command is only available on the Log Server. The operation checks permissions for the supplied administrator account from the Management Server to prevent unauthorized access to the logs.
	Enclose details in double quotes if they contain spaces.
	`Host` specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.
	`login` defines the user name for the account that is used for this operation. If this parameter is not defined, the user name root is used.
	`pass` defines the password for the user account.
	`format` defines the file format for the output file. If this parameter is not defined, the XML format is used.
	`i` defines the source from which the logs are exported. Can be a folder or a file. The processing recurses into subfolders.
	`o` defines the destination file where the logs are exported. If this parameter is not defined, the output is shown on screen.
	`f` defines a file that contains the filtering criteria you want to use for filtering the log data. You can export log filters individually in the Management Client through **Tools** > **Save for Command Line Tools** in the filter's right-click menu.
	`e` allows you to enter a filter expression manually (using the same syntax as exported filter files).
	`-h`, `-help`, or `-?` shows information about using the script.
	`-v` shows verbose output on the command execution.
	Example (exports logs from one full day to a file using a filter): `sgArchiveExport login=admin pass=abc123 i= C:\Program Files\Forcepoint\SMC \data \archive\firewall\year2011\month12\.\sgB.day01\ f= C:\Program Files\Forcepoint\SMC \export\MyExportedFilter.flp format=CSV o=MyExportedLogs.csv`

`sgBackupLogSrv`
`[pwd=<password>]`
`[path=<destpath>]`
`[nodiskcheck]`
`[comment=<comment>]`
`[nofsstorage]`
`[-h|--help]`
	Note
	For the SMC Appliance, use the `smca-backup` command.
	Creates a backup of Log Server configuration data.
	The backup file is stored in the `<installation directory>/backups/` directory.
	Twice the size of the log database is required on the destination drive. Otherwise, the operation fails.
	`pwd` enables encryption.
	`path` defines the destination path.
	`nodiskcheck` ignores the free disk check before creating the backup.
	`comment` allows you to enter a comment for the backup. The maximum length of a comment is 60 characters.
	`nofsstorage` creates a backup only of the Log Server configuration without the log data.
	`-h` or `--help` shows information about using the script.
	Also see `sgRestoreLogBackup`.

Command	Description

`sgBackupMgtSrv`
`[pwd=<password>]`
`[path=<destpath>]`
`[nodiskcheck]`
`[comment=<comment>]`
`[-h|--help]`
	Note
	For the SMC Appliance, use the `smca-backup` command.
	
	Creates a complete backup of the Management Server (including both the local configuration and the stored information in the configuration database). The backup file is stored in the `<installation directory>/backups/` directory.
	
	Twice the size of the Management Server database is required on the destination drive. Otherwise, the operation fails.
	
	`pwd` enables encryption.
	
	`path` defines the destination path.
	
	`nodiskcheck` ignores the free disk check before creating the backup.
	
	`comment` allows you to enter a comment for the backup. The maximum length of a comment is 60 characters.
	
	`-h` or `--help` shows information about using the script.
	
	Also see `sgRestoreMgtBackup` and `sgRecoverMgtDatabase`.

`sgCertifyLogSrv` `[host=<Management Server Address[\Domain]>`	Contacts the Management Server and creates a certificate for the Log Server to allow secure communications with other SMC components. Renewing an existing certificate does not require changing the configuration of any other SMC components. `host` specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used. `Domain` specifies the administrative Domain the Log Server belongs to if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used. Stop the Log Server before running this command. Restart the server after running this command.

`sgCertifyMgtSrv`
`[login=<login name>]`
`[pass=<password>]`
`[standby-server=<name of additional Management Server>]`
`[active-server=<IP address of active Management Server>]`
`[-nodisplay]`
`[-h|-help|-?]`
	Creates a certificate for the Management Server to allow secure communications between the SMC components. Renewing an existing certificate does not require changes on any other SMC components.
	
	In an environment with only one Management Server, or to certify the active Management Server, stop the Management Server before running the `sgCertifyMgtSrv` command. Run the command without parameters. Restart the Management Server after running this command.
	
	To certify an additional Management Server, stop the additional Management Server before running the `sgCertifyMgtSrv` command. The active Management Server must be running when you run this command. The management database is replicated to the additional Management Server during the certification. The additional Management Server must have a connection to the active Management Server when you run this command.
	
	`[login=<login name>]` defines the user name for the account that is used for this operation. If this parameter is not defined, the user name root is used.
	
	`[pass=<password>]` defines the password for the user account.
	
	`[standby-server]` specifies the name of the additional Management Server to be certified.
	
	`[active-server]` specifies the IP address of the active Management Server.
	
	`-nodisplay` sets a text-only console.
	
	`-h`, `-help`, or `-?` shows information about using the script.

Command	Description
`sgCertifyWebPortalSrv` `[host=<Management Server Address[\Domain]>]`	Contacts the Management Server and creates a certificate for the Web Portal Server to allow secure communications with other SMC components. Renewing an existing certificate does not require changing the configuration of any other SMC components. `host` specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used. `Domain` specifies the administrative Domain the Web Portal Server belongs to if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used. Stop the Web Portal Server before running this command. Restart the server after running this command.
`sgChangeMgtIPOnLogSrv <IP address>`	Changes the Management Server's IP address in the Log Server's local configuration to the IP address you give as a parameter. Use this command if you change the Management Server's IP address. Restart the Log Server service after running this command.
`sgChangeMgtIPOnMgtSrv <IP address>`	Changes the Management Server's IP address in the local configuration to the IP address you give as a parameter. Use this command if you change the Management Server's IP address. Restart the Management Server service after running this command.
`sgClient`	Starts a locally installed Management Client.
`sgCreateAdmin`	Creates an unrestricted (superuser) administrator account. The Management Server must be stopped before running this command.

Command	Description
`sgExport [host=<Management Server Address[\Domain]>]` `[login=<login name>]` `[pass=password]` `file=<file path and name>` `[type=<all|nw|ips|sv|rb|al|vpn>` `[name=<element name 1, element name 2, ...>]` `[recursion]` `[-system]` `[-h|-help|-?]`	Exports elements stored on the Management Server to an XML file. Enclose details in double quotes if they contain spaces. `host` specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used. `Domain` specifies the administrative Domain for this operation if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used. `login` defines the user name for the account that is used for this operation. If this parameter is not defined, the user name root is used. `pass` defines the password for the user account. `file` defines the name and location of the export .zip file. `type` specifies which types of elements are included in the export file: ■ `all` for all exportable elements ■ `nw` for network elements ■ `ips` for IPS elements ■ `sv` for services ■ `rb` for security policies ■ `al` for alerts ■ `vpn` for VPN elements. `name` allows you to specify by name the elements that you want to export. `recursion` includes referenced elements in the export, for example, the network elements used in a policy that you export. `-system` includes any system elements that are referenced by the other elements in the export. `-h`, `-help`, or `-?` shows information about using the script.

Command	Description

`sgHA`
`[host=<Management Server Address[\Domain]>]`
`[login=<login name>]`
`[pass=<password>]`
`[master=<Management Server used as master server for the operation>]`
`[-set-active]`
`[-set-standby]`
`[-check]`
`[-retry]`
`[-force]`
`[-restart]`
`[-h|-help|-?]`
	Controls active and standby Management Servers.
	If you want to perform a full database synchronization, use the `sgOnlineReplication` command.
	`host` specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.
	`Domain` specifies the administrative Domain for this operation if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used.
	`login` defines the user name for the account that is used for this operation. If this parameter is not defined, the user name root is used.
	`pass` defines the password for the user account.
	`master` defines the Management Server used as a master Management Server for the operation.
	`-set-active` activates and locks all administrative Domains.
	`-set-standby` deactivates and unlocks all administrative Domains.
	`-check` checks that the Management Server's database is in sync with the master Management Server.
	`-retry` retries replication if this has been stopped due to a recoverable error.
	`-force` enforces the operation even if all Management Servers are not in sync.
	Note
	This option can cause instability if used carelessly.
	`-restart` restarts the specified Management Server.
	`-h`, `-help`, or `-?` shows information about using the script.

`sgImport`
`[host=<Management Server Address[\Domain]>]`
`[login=<login name>]`
`[pass=<password>]`
`file=<file path and name>`
`[-replace_all]`
`[-h|-help|-?]`
	Imports Management Server database elements from an XML file.
	When importing, existing (non-default) elements are overwritten if both the name and type match.
	`host` specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.
	`Domain` specifies the administrative Domain for this operation if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used.
	`login` defines the user name for the account that is used for this operation. If this parameter is not defined, the user name root is used.
	`pass` defines the password for the user account.
	`file` defines the .zip file whose contents you want to import.
	`-replace_all` ignores all conflicts by replacing all existing elements with new ones.
	`-h`, `-help`, or `-?` shows information about using the script.

Command	Description

`sgImportExportUser`
`[host=<<Management Server Address[\Domain]>>]`
`[login=<login name>]`
`[pass=password]`
`action=<import|export>`
`file=<file path and name>`
`[-h|-help|-?]`
	Imports and exports a list of Users and User Groups in an LDIF file from or to a Management Server's internal LDAP database.
	To import User Groups, all User Groups in the LDIF file must be directly under the stonegate top-level group (dc=stonegate).
	CAUTION
	The user information in the export file is stored as plaintext. Handle the file securely.
	`host` specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.
	`Domain` specifies the administrative Domain for this operation if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used.
	`login` defines the user name for the account that is used for this operation. If this parameter is not defined, the user name `root` is used.
	`pass` defines the password for the user account.
	`action` defines whether users are imported or exported.
	`file` defines the file that is used for the operation.
	Example: `sgImportExportUser login=admin pass=abc123 action=export file=c:\temp\exportedusers.ldif`
	`-h`, `-help`, or `-?` shows information about using the script.

`sgInfo`
`SG_ROOT_DIR`
`FILENAME`
`[fast=<timestamp>]`
`[list]`
`[hprof=none|limited|all]`
`[-nolog]`
`[-client]`
`[-h|-help|-?]`
	Creates a .zip file that contains copies of configuration files and the system trace files.
	The resulting .zip file is stored in the logged on user's home directory. The file location is shown on the last line of screen output. Provide the generated file to support for troubleshooting purposes.
	Note
	On the SMC Appliance, you must always specify the path to the directory in which the .zip file is stored. The directory must be accessible from the account that you use to log on to the command line of the SMC Appliance.
	`SG_ROOT_DIR` SMC installation directory.
	`FILENAME` name of output file.
	`fast` collects only traces that changed after the specified time stamp. Enter the time stamp in milliseconds or in the format yyyy-MM-dd HH:mm:ss. No other information is collected, except for threaddumps.
	`[list]` only lists files. It does not create a .zip file or generate threaddumps.
	`hprof` defines whether hprof memory dump files are included.
	- `none` does not include hprof memory dump files.
	- `limited` includes only hprof memory dump files that are created with makeheap.
	- `all` includes memory dump files that are created with makeheap and java_pid.
	`-nolog` extended Log Server information is not collected.
	`-client` collects traces only from the Management Client.
	`-h`, `-help`, or `-?` shows information about using the script.

Command	Description

`sgOnlineReplication`
`[active-server=<name of active Management Server>]`
`[-nodisplay]`
`[-h|-help|-?]`
	Replicates the Management Server's database from the active Management Server to an additional Management Server.
	Stop the Management Server to which the database is replicated before running this command. Restart the Management Server after running this command.
	Use this script to replicate the database only in the following cases:
	■ The additional Management Server's configuration has been corrupted.
	■ In new SMC installations if the automatic database replication between the Management Servers has not succeeded.
	Otherwise, synchronize the database through the Management Client.
	CAUTION
	This script also has parameters that are for the internal use of the Management Server only. Do not use this script with any parameters other than the ones listed here.
	`active-server` specifies the IP address of the active Management Server from which the Management database is replicated.
	`-nodisplay` sets a text-only console.
	`-h`, `-help`, or `-?` shows information about using the script.

`sgReinitializeLogServer`	Creates a Log Server configuration if the configuration file has been lost. **Note** This script is located in `<installation directory>/bin/install`.
`sgRestoreArchive <ARCHIVE_DIR>`	Restores logs from archive files to the Log Server. This command is available only on the Log Server. `ARCHIVE_DIR` is the number of the archive directory (0–31) from where the logs will be restored. By default, only archive directory 0 is defined. The archive directories can be defined in the `<installation directory>/data/LogServerConfiguration.txt` file: `ARCHIVE_DIR_ xx=PATH`.

`sgRestoreLogBackup`
`[-pwd=<password>]`
`[-backup=<backup file name>]`
`[-nodiskcheck]`
`[-overwrite-syslog-template]`
`[-h|-help]`
	Restores the Log Server (logs or configuration files) from a backup file in the `<installation directory>/backups/` directory.
	`-pwd` defines a password for encrypted backup.
	`-backup` defines a name for the backup file.
	`-nodiskcheck` ignores the free disk check before backup restoration.
	`-overwrite-syslog-template` overwrites a syslog template file if found in the backup.
	`-h` or `-help` shows information about using the script.

Command	Description

`sgRestoreMgtBackup`
`[-pwd=<password>]`
`[-backup=<backup file name>]`
`[-import-license <license file name>]`
`[-nodiskcheck]`
`[-h|-help]`
	Restores the Management Server (database or configuration files) from a backup file in the `<installation directory>/backups/` directory.
	`-pwd` defines a password for encrypted backup.
	`-backup` defines a name for the backup file.
	`-import-license` specifies a license file to import during the backup restoration.
	`-nodiskcheck` ignores the free disk check before backup restoration.
	`-h` or `-help` shows information about using the script.

`sgRevert`	Reverts to the previous installation saved during the upgrade process. The previous installation can be restored at any time, even after a successful upgrade. **Note** This script is located in `<installation directory>/bin/uninstall`.
`sgShowFingerPrint`	Shows the CA certificate's fingerprint on the Management Server.
`sgStartLogSrv`	Starts the Log Server and its database.
`sgStartMgtDatabase`	Starts the Management Server's database. There is usually no need to use this script.
`sgStartMgtSrv`	Starts the Management Server and its database.
`sgStartWebPortalSrv`	Starts the Web Portal Server.
`sgStopLogSrv`	Stops the Log Server.
`sgStopMgtSrv`	Stops the Management Server and its database.
`sgStopMgtDatabase`	Stops the Management Server's database. There is usually no need to use this script.
`sgStopWebPortalSrv`	Stops the Web Portal Server.

`sgStopRemoteMgtSrv`
`[host=<Management Server address[\Domain]>]`
`[login=<login name>]`
`[pass=<password>]`
`[-h|-help|-?]`
	Stops the Management Server service when run without arguments.
	To stop a remote Management Server service, provide the arguments to connect to the Management Server.
	`host` is the Management Server's host name if not localhost.
	`login` is an SMC administrator account for the logon.
	`pass` is the password for the administrator account.
	`-h`, `-help`, or `-?` shows information about using the script.

Command	Description
`sgTextBrowser [host=<Management Server address[\Domain]>] [login=<login name>] [pass=<password>] [format=<CSV|XML>] [o=<output file>] [f=<filter file>] [e=<filter expression>] [m=<current|stored>] [limit=<maximum number of unique records to fetch>] [-h|-help|-?]`	Shows or exports current or stored logs. This command is available on the Log Server. Enclose the file and filter names in double quotes if they contain spaces. `host` defines the address of the Management Server used for checking the logon information. If this parameter is not defined, Management Server is expected to be on the same host where the script is run. If Domains are in use, you can specify the Domain the Log Server belongs to. If `domain` is not specified, the Shared Domain is used. `login` defines the user name for the account that is used for this export. If this parameter is not defined, the user name root is used. `pass` defines the password for the user account used for this operation. `format` defines the file format for the output file. If this parameter is not defined, the XML format is used. `o` defines the destination output file where the logs will be exported. If this parameter is not defined, the output is shown on screen. `f` defines the exported filter file that you want to use for filtering the log data. `e` defines the filter that you want to use for filtering the log data. Type the name as shown in the Management Client. `m` defines whether you want to view or export logs as they arrive on the Log Server (current) or logs stored in the active storage directory (stored). If this option is not defined, the current logs are used. `limit` defines the maximum number of unique records to be fetched. The default value is unlimited. `-h`, `-help`, or `-?` shows information about using the script.
`smca-agent` (SMC Appliance only)	SMC uses it to exchange configuration data between SMC and the operating system; not normally used by administrators. The agent configures the NTP and SNMP daemons and sets the logon and SSH banners.

`smca-backup`
(SMC Appliance only)
`[-pwd <password>]`
`[-comment <comment>]`
`[-nodiskcheck]`
`[-nofsstorage]`
`[-path <destination>]`
`[-log]`
`[-mgt]`
`[-h|--help]`
	Creates a configuration backup of the SMC Appliance operating system and includes an SMC backup.
	`-pwd <password>` enables the encryption of the backup file and sets the password.
	`-comment <comment>` adds a comment to the backup file name.
	`-nodiskcheck` turns off the available disk space check.
	`-nofsstorage` excludes the log files for the Log Server from the backup.
	`-path <destination>` specifies a path for backup file storage. The default directory for backups is `/usr/local/forcepoint/smc/backups`.
	`-log` creates a Log Server backup.
	`-mgt` creates a Management Server backup.
	`-h, --help` shows information about the command.
	Also see `sgRestoreLogBackup` and `sgRestoreMgtBackup`.

Command	Description

`smca-backup-remove`
(SMC Appliance only)
`[-f|--file]`
`[--force]`
`[--age <days>]`
`[--log]`
`[--mgt]`
`[-h|--help]`
	Removes old SMC Appliance backup files.
	`-f,--file` specifies the backup file to be removed.
	`--force` forces backup file delete without confirmation.
	`[--age <days>]` remove any backups older than the specified number of days. The default is 30 days.
	`[--log]` removes Log Server backups.
	`[--mgt]` removes Management Server backups.
	`-h, --help` shows information about the command.

`smca-cifs`
(SMC Appliance only)
`[add]`
`[remove]`
`[-n <name>]`
`[-s //<server>/<share>]`
`[-u <username>]`
`[-p <password>]`
`[-d <domain>]`
	Configures the mounting of remote CIFS file shares on the SMC Appliance.
	`add` adds the CIFS share.
	`remove` removes the CIFS share. Use with the name option.
	`-n <name>` specifies the name of the share.
	`-s //<server>/<share>` specifies the server or IP address of the share.
	`-u <username>` specifies the user name to authenticate with the CIFS server to get access to the share.
	`-p <password>` specifies the password on remote system.
	`-d <domain>` specifies the domain of the share.

`smca-restore`
(SMC Appliance only)
`[-pwd <password>]`
`[-nodiskcheck]`
`[-backup <filename>]`
`[-nosmca]`
`[-smcaonly]`
`[-overwrite-syslog-template]`
`[-h|-help]`
	Restores a backup on the SMC Appliance.
	`-pwd <password>` specifies the password for decrypting an encrypted backup file.
	`-nodiskcheck` turns off the available disk space check.
	`-backup <filename>` specifies the backup file name. If you do not specify the backup file name, you are prompted to select the backup file.
	`[-nosmca]` restores the Management Server or Log Server backup without restoring the SMC Appliance configuration
	`[-smcaonly]` restores the SMC Appliance configuration without restoring the Management Server or Log Server backup.
	`-overwrite-syslog-template` overwrites any existing syslog templates in the log backup file.
	`-h, --help` shows information about the command.

Command	Description

`smca-rsync`
(SMC Appliance only)
`[add]`
`[modify]`
`[remove]`
`[enable]`
`[disable]`
`[list]`
`[run]`
`[-t task_id]`
`[-i <source directory>]`
`[-o <destination directory>]`
`[-m <mode>]`
`[-h|-help]`
	Configures automated backup tasks. Typically used with the `smca-cifs` command to move backups off the appliance.
	`add` adds a backup task. You can specify an existing source and destination directories. If not specified, the default is `/usr/local/forcepoint/smc/backups/`.
	`modify` changes an existing backup task by its task ID. All attributes can be changed, except for the task ID. To change an attribute, use the appropriate option with a new value.
	`remove` removes an existing backup task by its task ID.
	`enable` enables an existing backup task by its task ID.
	`disable` disables an existing backup task by its task ID.
	`list` provides a list of all configured backup tasks.
	`run` runs all enabled backup tasks.
	`-t task_id` specifies the task ID. Use the list command to view the task IDs.
	`-i <source directory>` specifies the directory where the backups are stored when they are created. If omitted, the source directory defaults to the SMC backups directory `/usr/local/forcepoint/smc/backups/`.
	`-o <destination directory>` specifies the remote location to store the backups.
	`-m <mode>` specifies the rsync mode. You can indicate whether rsync appends or mirrors the source directory to the destination directory. Appending the directory means that existing files in the destination directory, that are not in the source directory or are newer than those files in the source directory, are not changed. If omitted, the mode defaults to append.
	`-h, --help` shows information about the command.

Command	Description

`smca-system`
(SMC Appliance only)
`[toggle]`
`[toggle-vcdrom]`
`[mirror [-n <name>]]`
`[snapshot [-C|--create] [-R|--restore] [-D, --delete] [-n <name>]]`
`[serial-number]`
`[fingerprint]`
`[toggle-console]`
`[bootloader-password [-s|--set] [-r|--remove]]`
`[netconfig]`
`[log-view [<filename>]]`
`[fips-config]`
`[-f]`
`[-h|-help]`
	Manages recovery snapshots, alternate partition mirroring, and changing system partition boot preference.
	`toggle` restarts the appliance to the alternate partition.
	`toggle-vcdrom` sets the appliance's default boot option to the vcdrom.
	`mirror` mirrors the active system to the alternate system. `-n <name>` specifies the name of the snapshot used for mirror operations.
	`snapshot` manages recovery snapshots.
	■ `-C, --create` creates a snapshot.
	■ `-D, --delete` deletes the snapshot.
	■ `-R, --restore` restores the snapshot.
	■ `-n <name>` specifies the name of the snapshot used for snapshot operations.
	`[serial-number]` shows the hardware serial number for the SMC Appliance.
	`[fingerprint]` shows the fingerprint for the CA used by the Management Client.
	`toggle-console` enables or disables the serial console on the SMC Appliance.
	`bootloader-password` manages the bootloader password for the SMC Appliance.
	■ `-s, --set` sets or changes the bootloader password.
	■ `-r, --remove` removes the bootloader password.
	`netconfig` sets up network-related configuration, such as IPv6 configuration.
	`log-view <filename>` shows the contents of the specified log file in the SMC Appliance log data directory `/var/log` or in any of the subdirectories of `/var/log`. `log-view -l` shows a list of all available log files.
	`fips-config` modifies the SMC Appliance configuration to support FIPS certification.
	`-f` forces the procedure, does not prompt for any confirmation.
	`-h, --help` shows information about the command.

`smca-user` (SMC Appliance only)	This utility is used by the SMC Appliance to keep user accounts in sync between the SMC and the operating system; not normally used by administrators.

Forcepoint NGFW Engine commands

There are commands that can be run on the command line on Firewall, Layer 2 Firewall, IPS engines, or Master NGFW Engines.

Note

Using the Management Client is the recommended configuration method, as most of the same tasks can be done through it.

Note

All command line tools that are available for single NGFW Engines are also available for Virtual NGFW Engines that have the same role. However, there is no direct access to the command line of Virtual NGFW Engines. Commands to Virtual NGFW Engines must be sent from the command line of the Master NGFW Engine using the `se-virtual-engine` command.

Some commands are only available when the NGFW Engine is in the Firewall (FW), Layer 2 Firewall (L2FW), or IPS engine (IPS) role.

Forcepoint NGFW command line tools

Command	Role	Description

`sg-blacklist`
`show [-v] [-f FILENAME ] |`
`add [`
`[-i FILENAME]|`
`[src IP_ADDRESS/MASK]`
`[src6 IPv6_ADDRESS/PREFIX]`
`[dst IP_ADDRESS/MASK]`
`[dst6 IPv6_ADDRESS/PREFIX]`
`[proto {tcp|udp|icmp|NUM}]`
`[srcport PORT {-PORT}]`
`[dstport PORT {-PORT}]`
`[duration NUM]`
`[ve VIRTUAL_ENGINE_ID]`
`] |`
`del [`
`[-i FILENAME]|`
`[src IP_ADDRESS/MASK]`
`[src6 IPv6_ADDRESS/PREFIX]`
`[dst IP_ADDRESS/MASK]`
`[dst6 IPv6_ADDRESS/PREFIX]`
`[proto {tcp|udp|icmp|NUM}]`
`[srcport PORT{-PORT}]`
`[dstport PORT{-PORT}]`
`[duration NUM]`
`[ve VIRTUAL_ENGINE_ID]`
`] |`
`iddel NODE_ID ID |`
`flush`
	FW
	L2FW
	IPS
		Used to view, add, or delete active blacklist entries.
		The blacklist is applied as defined in Access Rules.
		`show` shows the current active blacklist entries in format: `engine node ID | blacklist entry ID | (internal) | entry creation time | (internal) | address and port match | originally set duration | (internal) | (internal)`. Use the `-f` option to specify a storage file to view (`/data/blacklist/db_<number>`). The `-v` option adds operation's details to the output.
		`add` creates a blacklist entry. Enter the parameters or use the `-i` option to import parameters from a file.
		`del` deletes the first matching blacklist entry. Enter the parameters or use the `-i` option to import parameters from a file.
		`iddel` removes one specific blacklist entry on one specific NGFW Engine. `NODE_ID` is the ID of the NGFW Engine, `ID` is the blacklist entry's ID (as shown by the show command).
		`flush` deletes all blacklist entries.
		Add/Del Parameters:
		Enter at least one parameter. The default value is used for the parameters that you omit. You can also save parameters in a text file; each line in the file is read as one blacklist entry.
		`src` defines the source IP address and netmask to match. Matches any IP address by default.
		`src6` defines the source IPv6 and prefix length to match. Matches any IPv6 address by default.
		`dst` defines the destination IP address and netmask to match. Matches any IP address by default.
		`dst6` defines the destination IPv6 address and prefix length to match. Matches any IPv6 address by default.
		`proto` defines the protocol to match by name or protocol number. Matches all IP traffic by default.
		`srcport` defines the TCP/UDP source port or range to match. Matches any port by default.
		`dstport` defines the TCP/UDP destination port or range to match. Matches any port by default.
		`duration` defines in seconds how long the entry is kept. Default is 0, which cuts current connections, but is not kept.
		`ve` specifies the Virtual NGFW Engine on which the blacklist entry is created or deleted.
		Examples:
		`sg-blacklist add src 192.168.0.2/32 proto tcp dstport 80 duration 60`
		`sg-blacklist add -i myblacklist.txt`
		`sg-blacklist del dst 192.168.1.0/24 proto 47`

Command	Role	Description

`sg-bootconfig`
`[--primary-console=tty0|ttyS PORT,SPEED]`
`[--secondary-console=[tty0|ttyS PORT,SPEED]]`
`[--flavor=up|smp]`
`[--initrd=yes|no]`
`[--crashdump=yes|no|Y@X]`
`[--append=kernel options]`
`[--help]`
`apply`
	FW
	L2FW
	IPS
		Used to edit boot command parameters for future bootups.
		`--primary-console` defines the terminal settings for the primary console.
		`--secondary-console` defines the terminal settings for the secondary console.
		`--flavor` defines whether the kernel is uniprocessor or multiprocessor.
		`--initrd` defines whether Ramdisk is enabled or disabled.
		`--crashdump` defines whether kernel crashdump is enabled or disabled, and how much memory is allocated to the crash dump kernel (Y). The default is 24M. X must always be 16M.
		`--append` defines any other boot options to add to the configuration.
		`--help` shows usage information.
		`apply` applies the specified configuration options.

`sg-clear-all`
`[--help]`
`[--flash-defaults]`
`[--dry-run]`
`[--on-boot]`
`[--reboot | --shutdown]`
`[--fast] | --wipe <number>]`
`[--debug | --verbose]`
	FW
	L2FW
	IPS
		This command restores the factory default settings on the NGFW Engine.
		`[--help]` shows usage information.
		`[--flash-defaults]` assumes that the NGFW Engine has a flash data partition and a RAM spool partition.
		`[--dry-run]` exits without shutting down or restarting when command execution finishes.
		`[--on-boot]` indicates that NGFW Engine is starting up. This option is not intended to be used in normal command line usage.
		`[--reboot]` the NGFW Engine always restarts when command execution finishes.
		`[--shutdown]` the NGFW Engine always shuts down when command execution finishes.
		`[--fast]` runs a minimal, non-interactive clear for testing purposes.
		`[--wipe <number>]` globally specifies the number of times to wipe partitions.
		`[--debug]` shows full debug messages during command execution.
		`[--verbose]` shows additional informational messages during command execution.
		 
		Note
		If you run the command without specifying any options, the NGFW Engine requests confirmation before restarting. When the NGFW Engine restarts, you are prompted to select the system restore options.
		After using this command, you can reconfigure the NGFW Engine using the `sg-reconfigure` command.

Command	Role	Description

`sg-cluster`
`[-v Virtual NGFW Engine ID]`
`[status [-c SECONDS]]`
`[versions]`
`[online]`
`[lock-online]`
`[offline]`
`[lock-offline]`
`[standby]`
`[safe-offline]`
`[force-offline]`
	FW
	L2FW
	IPS
		Shows or changes the status of the node.
		`-v` (Master NGFW Engine only) specifies the ID of the Virtual NGFW Engine on which to execute the command.
		`status` shows cluster status. When `-c SECONDS` is used, the status is shown continuously with the specified number of seconds between updates.
		`version` shows the NGFW Engine software versions of the nodes in the cluster.
		`online` sends the node online.
		`lock-online` sends the node online and keeps it online, even if another process tries to change its state.
		`offline` sends the node offline.
		`lock-offline` sends the node offline and keeps it offline, even if another process tries to change its state.
		`standby` sets an active node to standby.
		`safe-offline` sets the node to offline only if there is another online node.
		`force-offline` sets the node online regardless of state or any limitations. Also sets all other nodes offline.

`sg-contact-mgmt`	FW L2FW IPS	Used for establishing a trust relationship with the Management Server as part of NGFW Engine installation or reconfiguration (see `sg-reconfigure`). The NGFW Engine contacts the Management Server using the one-time password created when the NGFW Engine's initial configuration is saved.
`sg-diagnostics [-s|-u] -f <facility_number>`	FW L2FW IPS	Enables or disables diagnostics for the specified facility. When enabled, diagnostic information for the specified facility is included in the log data. `-f <facility_number>` specifies the facility for which to enable diagnostics. Use the `sg-logger -s` command to get a list of facility numbers. `-s` enables diagnostics. `-u` disables diagnostics. When you run the command without `-s` or `-u`, the output shows the current value for the specified facility.

Command	Role	Description

`sg-dynamic-routing`
`[start]`
`[stop]`
`[restart]`
`[force-reload]`
`[backup <file>]`
`[restore <file>]`
`[sample-config]`
`[route-table]`
`[info]`
	FW	`start` starts the Quagga routing suite.
		`stop` stops the Quagga routing suite and flushes all routes made by zebra.
		`restart` restarts the Quagga routing suite.
		`force-reload` forces reload of the saved configuration.
		`backup` backs up the current configuration to a compressed file.
		`restore` restores the configuration from the specified file.
		`sample-config` creates a basic configuration for Quagga.
		`route-table` prints the current routing table.
		`info` shows the help information for the `sg-dynamic-routing` command, and detailed information about Quagga suite configuration with vtysh.

`sg-ipsec -d`
`[-u <username[@domain]> |`
`-si <session id>|`
`-ck <ike cookie> |`
`-tri <transform id> |`
`-ri <remote ip> |`
`-ci <connection id>]`
	FW	Deletes VPN-related information (use the `vpntool` command to view the information). Option `-d` (for delete) is mandatory.
		`-u` deletes the VPN session of the named VPN client user. You can enter the user account in the form `<user_name@domain>` if there are several user storage locations (LDAP domains).
		`-si` deletes the VPN session of a VPN client user based on session identifier.
		`-ck` deletes the IKE SA (Phase one security association) based on IKE cookie.
		`-tri` deletes the IPSEC SAs (Phase two security associations) for both communication directions based on transform identifier.
		`-ri` deletes all SAs related to a remote IP address in site-to-site VPNs.
		`-ci` deletes all SAs related to a connection identifier in site-to-site VPNs.

Command	Role	Description

`sg-log-view`
`-h | --help`
`-c CONFIGURATION_FILE`
`-C | --show-configuration`
`-N | --show-field-names`
`-A | --alerts`
`-o {list|table|json|json-pretty} | --output-format {list|table|json|json-pretty}`
`-f | --follow`
`-t TABLE_FIELDS [TABLE_FIELDS ...] | --table-fields TABLE_FIELDS [TABLE_FIELDS ...]`
`-a ADD_TABLE_FIELDS [ADD_TABLE_FIELDS ...] | --add-table-fields ADD_TABLE_FIELDS [ADD_TABLE_FIELDS ...]`
`-r REMOVE_TABLE_FIELDS [REMOVE_TABLE_FIELDS ...] | --remove-table-fields REMOVE_TABLE_FIELDS [REMOVE_TABLE_FIELDS ...]`
`-I | --add-event-id-table-field`
`-i EVENT_IDS [EVENT_IDS ...] | --event-ids EVENT_IDS [EVENT_IDS ...]`
`-s START_DATE | --start-date START_DATE`
`-e END_DATE | --end-date END_DATE`
`-F FILTERS [FILTERS ...] | --filters FILTERS [FILTERS ...]`
`--input-file-format {binary|json}`
`--log-files [LOG_FILES [LOG_FILES ...]]`
`--timestamp-type {date|integer}`
`-S | --show-log-counter`
	FW
	L2FW
	IPS
		If you have saved copies of the most recent log and alert entries locally on the NGFW Engine, allows you to browse log and alert entries on the command line of the NGFW Engine.
		`-h | --help` shows usage information.
		`-c` specifies a configuration file for viewing stored log entries. If you do not specify a configuration file in this command, the `LOG_VIEW_CONF` environment variable specifies the configuration file. If no configuration file is specified in the `LOG_VIEW_CONF` variable, the default configuration is used.
		`-C | --show-configuration` shows the active configuration.
		`-N | --show-field-names` shows all available log field names.
		`-A | --alerts` shows alert entries instead of log entries.
		`-o | --output-format` specifies the output format for log entries. The default is table.
		`-f | --follow` shows log entries in real time as they are generated.
		`-t | --table-fields` shows the specified fields in a table view. You can specify the width and position of the field in the table using numbers and semicolons. For example, `situation:40:3`.
		`-a | --add-table-fields` adds the specified fields to the table view. You can specify the width and position of the field in the table using numbers and semicolons. For example, `situation:40:3`.
		`-r | --remove-table-fields` removes the specified fields from the table view.
		`-I | --add-event-id-table-field` adds `event_id` as the first log field in the table view.
		`-i | --event-ids` shows details about the specified events (event ids) in a list view.
		`-s | --start-date` shows log entries starting from the specified date.
		`-e | --end-date` shows log entries ending on the specified date.
		`-F | --filters` specifies log filters as either a simple filter string or a complete JSON filter string.
		`--input-file-format` specifies the input log file format. The default is binary.
		`--log-files` specifies the log files to show. If you do not specify a log file, all available log files found in the specified log directories are shown.
		`--timestamp-type` shows timestamp values as dates or integers. The default is date.
		`-S | --show-log-counter` shows log counters in table and list views.

Command	Role	Description

`sg-logger`
`-f FACILITY_NUMBER`
`-t TYPE_NUMBER`
`[-e EVENT_NUMBER]`
`[-i "INFO_STRING"]`
`[-s]`
`[-h]`
	FW
	L2FW
	IPS
		Used in scripts to create log messages with the specified properties.
		`-f` defines the facility for the log message.
		`-t` defines the type for the log message.
		`-e` defines the log event for the log message. The default is `0 (H2A_LOG_EVENT_UNDEFINED)`.
		`-i` defines the information string for the log message.
		`-s` dumps information about option numbers to stdout
		`-h` shows usage information.

`sg-raid`
`[-status] [-add] [-re-add]`
`[-force] [-help]`
	FW
	L2FW
	IPS
		Configures a new hard drive.
		This command is only for Forcepoint NGFW appliances that support RAID (Redundant Array of Independent Disks) and have two hard drives.
		`-status` shows the status of the hard drive.
		`-add` adds a new empty hard drive. Use `-add -force` if you want to add a hard drive that already contains data and you want to overwrite it.
		`-re-add` adds a hard drive that is already partitioned. This command prompts for the drive and partition for each degraded array. Use `-re-add -force` if you want to check all arrays.
		`-help` shows usage information.

`sg-reconfigure`
`[--maybe-contact]`
`[--no-shutdown]`
`[--stop-autocontact]`
	FW
	L2FW
	IPS
		Starts the NGFW Configuration Wizard. Used for reconfiguring the node manually.
		CAUTION
		This script also has parameters that are for the internal use of the NGFW Engine only. Do not use this script with any parameters other than the ones listed here.
		`--maybe-contact` contacts the Management Server if requested. This option is only available on Firewalls.
		`--no-shutdown` allows you to make limited configuration changes on the node without shutting it down. Some changes might not be applied until the node is rebooted.
		`--stop-autocontact` (unconfigured Forcepoint NGFW appliances with valid POS codes only) prevents the NGFW Engine from contacting the installation server for plug-and-play configuration when it reboots.

`sg-selftest [-d] [-h]`	FW	Runs cryptography tests on the NGFW Engine. `-d` runs the tests in debug mode. `-h` shows usage information.
`sg-status [-l] [-h]`	FW L2FW IPS	Shows information about the NGFW Engine status. `-l` shows all available information about NGFW Engine status. `-h` shows usage information.

Command	Role	Description

`sg-toggle-active`
`SHA1 SIZE |`
`--force [--debug ]`
	FW
	L2FW
	IPS
		Switches the NGFW Engine between the active and the inactive partition.
		This change takes effect when you reboot the NGFW Engine.
		You can use this command, for example, if you have upgraded an NGFW Engine and want to switch back to the earlier NGFW Engine version. When you upgrade the NGFW Engine, the active partition is switched. The earlier configuration remains on the inactive partition. To see the currently active (and inactive) partition, see the directory listing of `/var/run/stonegate` (`ls -l /var/run/stonegate`).
		The `SHA1` option is used to verify the signature of the inactive partition before changing it to active. If you downgrade the NGFW Engine, check the checksum and the size of the earlier upgrade package by extracting the signature and size files from the `sg_engine_[version.build]_i386.zip` file.
		`--debug` reboots the NGFW Engine with the debug kernel.
		`--force` switches the active configuration without first verifying the signature of the inactive partition.

`sg-upgrade`	FW	Upgrades the node by rebooting from the installation DVD. Alternatively, the node can be upgraded remotely using the Management Client.
`sg-version`	FW L2FW IPS	Shows the software version and build number for the node.

`se-virtual-engine`
`-l | --list`
`-v <Virtual NGFW Engine ID>`
`-e | --enter`
`-E "<command [options]>"`
`-h | --help`
	FW	
		Note
		Master NGFW Engine only.
		Used to send commands to Virtual Firewalls from the command line of the Master NGFW Engine.
		All commands that can be used for the Firewall role can also be used for Virtual Firewalls.
		`-l` or `--list` list the active Virtual NGFW Engines.
		`-v` specifies the ID of the Virtual NGFW Engine on which to execute the command.
		`-e` or `--enter` enters the command shell for the Virtual NGFW Engine specified with the `-v` option. To exit the command shell, type `exit`.
		`-E` executes the specified command on the Virtual NGFW Engine specified with the `-v` option.
		`-h` or `--help` shows usage information.

Command	Role	Description

`sginfo`
`[-f]`
`[-d]`
`[-s]`
`[-p]`
`[--]`
`[--help]`
	FW
	L2FW
	IPS
		Gathers system information you can send to Forcepoint support.
		Use this command only when instructed to do so by Forcepoint support.
		`-f` forces sgInfo even if the configuration is encrypted.
		`-d` includes core dumps in the sgInfo file.
		`-s` includes slapcat output in the sgInfo file.
		`-p` includes passwords in the sgInfo file (by default passwords are erased from the output).
		`--` creates the sgInfo file without showing the progress.
		`--help` shows usage information.

The following table lists some general Linux operating system commands that can be useful in running your NGFW Engines. Some commands can be stopped by pressing **Ctrl+C**.

General command line tools on NGFW Engines

Command	Description
`dmesg`	Shows system logs and other information. Use the `-h` option to see usage.
`halt`	Shuts down the system.
`ip`	Shows IP address information. Type the command without options to see usage. Example: type `ip addr` for basic information about all interfaces.
`ping`	Tests connectivity with ICMP echo requests. Type the command without options to see usage.
`ps`	Reports the status of running processes.
`reboot`	Reboots the system.
`scp`	Secure copy. Type the command without options to see usage.
`sftp`	Secure FTP. Type the command without options to see usage.
`ssh`	SSH client (for opening a terminal connection to other hosts). Type the command without options to see usage.
`tcpdump`	Gives information about network traffic. Use the `-h` option to see usage. You can also analyze network traffic by creating tcpdump files from the Management Client with the Traffic Capture feature.
`top`	Shows the top CPU processes taking most processor time. Use the `-h` option to see usage.

Command	Description
`traceroute`	Traces the route packets take to the specified destination. Type the command without options to see usage.
`vpntool`	Shows VPN information and allows you to issue some basic commands. Type the command without options to see usage.

Server Pool Monitoring Agent commands

You can test and monitor the Server Pool Monitoring Agents on the command line.

Server Pool Monitoring Agent commands

Command	Description

`agent`
`[-v level]`
`[-c path]`
`[test [files]]`
`[syntax [files]]`
	(Windows only) Allows you to test different configurations before activating them.
	`-v` sets the verbosity level. The default level is 5. Levels 6–8 are for debugging where available.
	`-c` uses the specified path as the first search directory for the configuration.
	`test` runs in the test mode - status queries do not receive a response. If you specify the files, they are used for reading the configuration instead of the default files.
	`syntax` checks the syntax in the configuration file. If no files are specified, the default configuration files are checked.

`sgagentd [-d]`
`[-v level]`
`[-c path]`
`[test [files]]`
`[syntax [files]]`
	(Linux only) Allows you to test different configurations before activating them.
	`-d` means Don't Fork as a daemon. All log messages are printed to stdout or stderr only.
	`-v` sets the verbosity level. The default level is 5. Levels 6–8 are for debugging where available.
	`-c` uses the specified path as the first search directory for the configuration.
	`test` runs in the test mode - status queries do not receive a response. If you specify the files, they are used for reading the configuration instead of the default files. The output is directed to syslog or eventlog instead of the console where the command was run unless you use the `-d` option.
	`syntax` checks the syntax in the configuration file. If no files are specified, the default configuration files are checked. The output is directed to syslog or eventlog instead of the console where the command was run unless you use the `-d` option.

Command	Description

`sgmon`
`[status|info|proto]`
`[-p port]`
`[-t timeout]`
`[-a id]`
`host`
	Sends a UDP query to the specified host and waits for a response until received, or until the timeout limit is reached. The request type can be defined as a parameter. If no parameter is given, status is requested. The commands are:
	`status` queries the status.
	`info` queries the agent version.
	`proto` queries the highest supported protocol version.
	`-p` connects to the specified port instead of the default port.
	`-t` sets the timeout (in seconds) to wait for a response.
	`-a` acknowledge the received log messages up to the specified id. Each response message has an id, and you can acknowledge more than one message at a given time by using the id parameter. Messages acknowledged by sgmon will no longer appear in the firewall logs.
	`host` is the IP address of the host to connect to. To get the status locally, you can give localhost as the host argument. This parameter is mandatory.

Appendix C

Installing SMC Appliance software on a virtualization platform

Contents

You can install the SMC Appliance software as a virtual machine on virtualization platforms such as VMware ESX. After installation, you can patch and upgrade the SMC Appliance in the same way as a purpose-built SMC Appliance.

Hardware requirements for installing SMC Appliance software on a virtualization platform

There are some hardware and software requirements when you run SMC Appliance software on a virtualization platform.

For more information, see the Release Notes.

Install SMC Appliance software using an .iso file

Use an .iso file of the SMC Appliance software to install the SMC Appliance on the VMware ESX virtualization platform.

Steps

1) Create the virtual machine and configure it according to your requirements.
2) Download the license at https://stonesoftlicenses.forcepoint.com.
3) Download the .iso installation file at https://support.forcepoint.com.
4) Connect the DVD drive of the virtual machine to the .iso file.

5) Restart the virtual machine.

6) When the NGFW SMC Appliance installer starts, type `I`.

7) To start the SMC Appliance installation, type `Erase` and press **Enter**.

8) When the SMC Appliance software installation is complete, type `Y` to restart the virtual machine.

Next steps

Continue the SMC Appliance installation by configuring the operating system settings on the command line of the SMC Appliance.

Related tasks

Install the SMC Appliance on page 54

Appendix D

Installing Forcepoint NGFW on a virtualization platform

Contents

You can install the Forcepoint NGFW software as a virtual machine on virtualization platforms such as VMware ESX or KVM.

The same Forcepoint NGFW software can be used in the Firewall/VPN role, IPS role, or Layer 2 Firewall role. The engine role is selected during the initial configuration of the engine.

Hardware requirements for installing Forcepoint NGFW software on a virtualization platform

There are some hardware and software requirements, and configuration limitations when you run Forcepoint NGFW software on a virtualization platform.

For more information, see the Release Notes.

Install Forcepoint NGFW software using an .iso file

Use an .iso file of the Forcepoint NGFW software to install Forcepoint NGFW on VMware ESX, KVM, or Microsoft Hyper-V virtualization platforms.

Only NGFW Engines in the Firewall/VPN role are supported on the Microsoft Hyper-V virtualization platform.

Steps

1) Create the virtual machine and configure it according to your requirements.

2) (IPS and Layer 2 Firewall only) Configure the virtual switches to which the IPS or Layer 2 Firewall inline interfaces are connected:

   a) Create a port group, then assign **All** (4095) as the **VLAN ID**.

b) Enable the use of **Promiscuous Mode**.

3) Download the license at https://stonesoftlicenses.forcepoint.com.

4) Download the .iso installation file at https://support.forcepoint.com.

5) Connect the DVD drive of the virtual machine to the .iso file.

6) Restart the virtual machine.
The License Agreement appears.

7) Type `YES`, then press **Enter** to accept the license agreement and continue with the configuration.

8) Select the type of installation:
   - Type `1` for the normal **Full Install**.
   - Type `2` for the **Full Install in expert mode** if you want to partition the hard disk manually.

9) Enter the number of processors:
   - For a uniprocessor system, type `1`, then press **Enter**.
   - For a multiprocessor system, type `2`, then press **Enter**.

10) Continue in one of the following ways:
   - If you selected **Full Install**, type `YES`, then press **Enter** to accept automatic hard disk partitioning.
   - If you selected **Full Install in expert mode**, install the engine in expert mode.

Result

The installation process starts.

Appendix E

Installing Forcepoint NGFW software on third-party hardware

Contents

You can install the Forcepoint NGFW software on third-party hardware that meets the hardware requirements.

Hardware requirements for installing Forcepoint NGFW on third-party hardware

There are some basic hardware requirements when you run Forcepoint NGFW on third-party hardware.

For more information, see the Release Notes.

For information about supported Ethernet interface types and adapters, see Knowledge Base article 9721.

CAUTION

Check that the Automatic Power Management (APM) and Advanced Configuration and Power Interface (ACPI) settings are disabled in BIOS. Otherwise, the engine might not start after installation or can shut down unexpectedly.

CAUTION

The hardware must be dedicated to the Forcepoint NGFW. No other software can be installed on it.

Hardware drivers

We recommend using the listed approved drivers supported by Forcepoint NGFW.

Tested network interface card drivers included in the kernel of Forcepoint NGFW are listed in the following table. These drivers have been tested for use in Forcepoint NGFW.

Tested network interface card drivers

Driver	Version	Description
e1000e.ko	3.2.6-k	Intel® PRO/1000 Network Driver
e1000x.ko	7.3.21-k8-NAPI	Intel® PRO/1000 Network Driver
i40e.ko	2.3.6+sg3	Intel® 40-10 Gigabit Ethernet Connection Network Driver
igb.ko	5.3.5.22+sg2	Intel® Gigabit Ethernet Linux Driver
ixgbe.ko	5.2.4+sg11	Intel® 10GbE PCI Express Linux Network Driver
virtio_net.ko	No version	Virtio network driver
vmxnet3.ko	1.4.a.0-k	VMware vmxnet3 virtual NIC driver
xen-netfront.ko	No version	Xen virtual network device frontend

Other network interface card drivers included in the kernel of Forcepoint NGFW are listed in the following table. All drivers are the driver version that is included in the standard Linux 4.14.138 kernel.

Note

These drivers have not been tested for use in Forcepoint NGFW.

Other network interface card drivers

Driver	Description
3c59x.ko	3Com 3c59x/3c9xx Ethernet driver
8139cp.ko	RealTek RTL-8139C+ series 10/100 PCI Ethernet Driver
8139too.ko	RealTek RTL-8139 Fast Ethernet Driver
8390.ko	No description
acenic.ko	AceNIC/3C985/GA620 Gigabit Ethernet Driver
amd8111e.ko	AMD8111 based 10/100 Ethernet Controller. Driver Version 3.0.7
atl1.ko	Atheros L1 Gigabit Ethernet Driver
atl1e.ko	Atheros 1000M Ethernet Network Driver
b44.ko	Broadcom 44xx/47xx 10/100 PCI Ethernet Driver
be2net.ko	Emulex OneConnect NIC Driver 10.2u
bnx2.ko	Broadcom NetXtreme II BCM5706/5708/5709/5716 Driver
bnx2x.ko	Broadcom NetXtreme II BCM57710/57711/57711E/57712/ 57712_MF/57800/57800_MF/57810/ 57810_MF/57840/57840_MF Driver
tg3.ko	Broadcom Tigon3 Ethernet Driver
cxgb.ko	Chelsio 10 Gb Ethernet Driver
cxgb3.ko	Chelsio T3 Network Driver
cxgb4.ko	Chelsio T4/T5 Network Driver
dl2k.ko	D-Link DL2000-based Gigabit Ethernet Adapter

Driver	Description
dmfe.ko	Davicom DM910X fast Ethernet Driver
e100.ko	Intel® PRO/100 Network Driver
epic100.ko	SMC 83c170 EPIC series Ethernet Driver
fealnx.ko	Myson MTD-8xx 100/10M Ethernet PCI Adapter Driver
forcedeth.ko	Reverse Engineered nForce Ethernet Driver
hamachi.ko	Packet Engines 'Hamachi' GNIC-II Gigabit Ethernet Driver
hp100.ko	HP CASCADE Architecture Driver for 100VG-AnyLan Network Adapters
i40e_ik.ko	Intel® Ethernet Connection XL710 Network Driver
igb_ik.ko	Intel® Gigabit Ethernet Network Driver
ipg.ko	IC Plus IP1000 Gigabit Ethernet Adapter Linux Driver
ixgb.ko	Intel® PRO/10GbE Network Driver
ixgbe_ik.ko	Intel® 10 gigabit PCI Express Network Driver
mdio.ko	Generic support for MDIO-compatible transceivers
mii.ko	MII hardware support library
mlx4_core.ko	Mellanox ConnectX HCA low-level driver
mlx4_en.ko	Mellanox ConnectX HCA Ethernet Driver
myri10ge.ko	Myricom 10G driver (10GbE)
natsemi.ko	National Semiconductor DP8381x series PCI Ethernet Driver
ne2k-pci.ko	PCI NE2000 clone driver
netxen_nic.ko	QLogic/NetXen (1/10) GbE Intelligent Ethernet Driver
niu.ko	NIU Ethernet Driver
ns83820.ko	National Semiconductor DP83820 10/100/1000 driver
pcnet32.ko	Driver for PCnet32 and PCnetPCI based ether cards
qla3xxx.ko	QLogic ISP3XXX Network Driver v2.03.00-k5
r6040.ko	RDC R6040 NAPI PCI Fast Ethernet Driver
r8169.ko	RealTek RTL-8169 Gigabit Ethernet Driver
s2io.ko	No description
sc92031.ko	Silan SC92031 PCI Fast Ethernet Adapter Driver
sis190.ko	SiS sis190/191 Gigabit Ethernet Driver
sis900.ko	SiS 900 PCI Fast Ethernet Driver
skge.ko	SysKonnect Gigabit Ethernet Driver
sky2.ko	Marvell Yukon 2-Gigabit Ethernet Driver
starfire.ko	Adaptec Starfire Ethernet Driver

Driver	Description
sundance.ko	Sundance Alta Ethernet driver
sungem.ko	Sun GEM Gbit Ethernet Driver
sunhme.ko	Sun HappyMealEthernet(HME) 10/100baseT Ethernet Driver
tehuti.ko	Tehuti Networks® Network Driver
tg3.ko	Broadcom Tigon3 ethernet driver
tulip.ko	Digital 21*4* Tulip Ethernet Driver
typhoon.ko	3Com Typhoon Family (3C990, 3CR990, and variants)
uli526x.ko	ULi M5261/M5263 fast Ethernet Driver
via-rhine.ko	VIA Rhine PCI Fast Ethernet driver
via-velocity.ko	VIA Networking Velocity Family Gigabit Ethernet Adapter Driver
winbond-840.ko	Winbond W89c840 Ethernet driver
yellowfin.ko	Packet Engines Yellowfin G-NIC Gigabit Ethernet Driver

SCSI drivers included in the kernel of Forcepoint NGFW are listed in the following table. All drivers are the driver version that is included in the standard Linux 4.14.138 kernel.

Note

Not all included drivers have been tested for use in Forcepoint NGFW.

SCSI drivers

Driver	Description
3Ware 9xxx SATA_RAID	[CONFIG_SCSI_3W_9XXX]
Adaptec / IBM ServeRAID	[CONFIG_SCSI_IPS]
Adaptec AACRAID	[CONFIG_SCSI_AACRAID]
Adaptec I2O RAID	[CONFIG_SCSI_DPT_I2O]
Adaptec SAS/SATA 3Gb/s	[CONFIG_SCSI_AIC94X]
Adaptec Ultra160	[CONFIG_SCSI_AIC7XXX]
BusLogic MultiMaster and FlashPoint SCSI	[CONFIG_SCSI_BUSLOGIC]
Domex DMX3191D SCSI	[CONFIG_SCSI_DMX3191D]
Fusion MPT ScsiHost for FC/SPI/SAS	[CONFIG_FUSION_FC/SPI/SAS]
Initio INIA100 SCSI	[CONFIG_SCSI_INIA100]
Intel PIIX/ICH PATA/SATA	[CONFIG_ATA_PIIX]
LSI Logic MegaRAID (Legacy)	[CONFIG_MEGARAID_LEGACY]
LSI Logic MegaRAID (NEWGEN)	[CONFIG_MEGARAID_NEWGEN]
LSI Logic MegaRAID (SAS)	[CONFIG_MEGARAID_SAS]
NVIDIA nForce SATA	[CONFIG_SATA_NV]

Driver	Description
Pacific Digital ADMA	[CONFIG_PDC_ADMA]
Promise SATA	[CONFIG_SATA_SX4]
Promise SATA TX2/TX4	[CONFIG_SATA_PROMISE]
QLogic IPS2x00	[CONFIG_SCSI_QLA2XXX]
QLogic ISP1240/1x80/1x160/1020/1040 SCSI	[CONFIG_SCSI_QLOGIC_1280]
ServerWorks / Apple K2 SATA	[CONFIG_SATA_SVW]
Silicon Image 3124/3132 SATA	[CONFIG_SATA_SIL24]
Silicon Image SATA	[CONFIG_SATA_SIL]
Silicon Integrated Systems SATA	[CONFIG_SATA_SIS]
Symbios/LSI logic 53C8XX/53C101	[CONFIG_SCSI_SYM53C8XX_2]
Tekram DC390(T) PCI SCSI	[CONFIG_SCSI_DC390T]
ULi Electronics SATA	[CONFIG_SATA_ULI]
VIA SATA	[CONFIG_SATA_VIA]
Vitesse VSC7174 SATA	[CONFIG_SATA_VITESSE]
Vortex GDT Disk Array / Intel Storage RAID	[CONFIG_SCSI_GDTH]

Block device drivers included in the kernel of Forcepoint NGFW are listed in the following table. All drivers are the driver version that is included in the standard Linux 4.14.138 kernel.

Note

Not all included drivers have been tested for use in Forcepoint NGFW.

Block device drivers

Driver
3ware Storage controller
AMD / NS 5535 IDE
CMD-Technologies CMD640 IDE
CMD-Technologies CMD64x IDE
Compaq Smart Array 5xxx
Compaq SMART2 Array
Cyrix / NS 5530 IDE
Highpoint 366 IDE
Intel PIIX IDE
ITE 8211 IDE/8212 IDE RAID
Mylec DAC960 / AcceleRAID / eXtremeRAID PCI RAID
RZ1000 IDE

Driver
Serverworks OSB4 / CSB5 / CSB6
Silicon Image SiL IDE

Start the Forcepoint NGFW installation on third-party hardware

After configuring the engine elements in the SMC, begin installing the Forcepoint NGFW software on your own hardware.

Before you begin

Before you start installing the Forcepoint NGFW software, make sure that you have the initial configuration and a one-time password for management contact for each engine. These items are generated in the SMC.

CAUTION

Installing the Forcepoint NGFW software deletes all existing data on the hard disk.

Depending on your order, you might have received ready-made SMC and Forcepoint NGFW software DVDs. If the DVDs are not included in the order, you must first create them.

Steps

1) Insert the engine installation DVD into the drive and restart the system.
   The License Agreement appears.

2) Type `YES` and press **Enter** to accept the license agreement and continue with the configuration.

3) Select the type of installation:
   - Type `1` for the normal **Full Install**.
   - Type `2` for the **Full Install in expert mode** if you want to partition the hard disk manually.

4) Enter the number of processors:
   - For a uniprocessor system, type `1` and press **Enter**.
   - For a multiprocessor system, type `2` and press **Enter**.

5) Continue in one of the following ways:
   - If you selected **Full Install**, type `YES` and press **Enter** to accept automatic hard disk partitioning.
   - If you selected **Full Install in expert mode**, install the engine in expert mode.

Result

The installation process starts.

Install Forcepoint NGFW in expert mode

You can install Forcepoint NGFW in expert mode if you want to partition the hard disk manually. If you are unfamiliar with partitioning hard disks in Linux, use the normal installation process.

CAUTION

When using the command prompt, use the `reboot` command to reboot and `halt` command to shut down the node. Do not use the `init` command. You can also reboot the node using the Management Client.

Partition the hard disk in expert mode

Typically, you need five partitions for an engine.

CAUTION

Partitioning deletes all existing data on the hard disk.

Steps

1) If you are asked whether you want to create an empty partition table, type `y` to continue.

2) When prompted, press **Enter** to continue.
   The partition table is displayed.

3) Create the partitions for the engine as follows:

Partition	Flags	Partition type	File system type	Size	Description
Engine root A	bootable	Primary	Linux	1000 MB	The bootable root partition for the engine element.
Engine root B		Primary	Linux	1000 MB	Alternative root partition for the engine element. Used for the engine upgrade.
Swap		Logical	Linux swap	Twice the size of physical memory.	Swap partition for the engine element.
Data		Logical	Linux	500 MB or more	Used for the boot configuration files and the root user's home directory.
Spool		Logical	Linux	All remaining free disk space.	Used for spooling.

4) Check that the partition table information is correct.

5) Select **Write** to commit the changes and confirm by typing yes.

6) Select **Quit** and press **Enter**.

Allocate partitions in expert mode

After partitioning the hard disk, assign the partitions for the engine.

Steps

1) Check that the partition table is correct. Type `yes` to continue.

2) Using the partition numbers of the partition table, assign the partitions. For example:
   - For the engine root A partition, type `1`.
   - For the engine root B partition, type `2`.
   - For the swap partition, type `5`.
   - For the data partition, type `6`.
   - For the spool partition, type `7`.

3) Check the partition allocation and type yes to continue.
   The engine installation starts.

4) When installation is complete, remove the DVD from the system and press **Enter** to reboot.

Related tasks

Configure Forcepoint NGFW software using automatic configuration on page 187
Using the NGFW Configuration Wizard on page 188

Appendix F

Example network (Firewall/VPN)

Contents

This example gives you a better understanding of how Forcepoint NGFW in the Firewall/VPN role fits into a network.

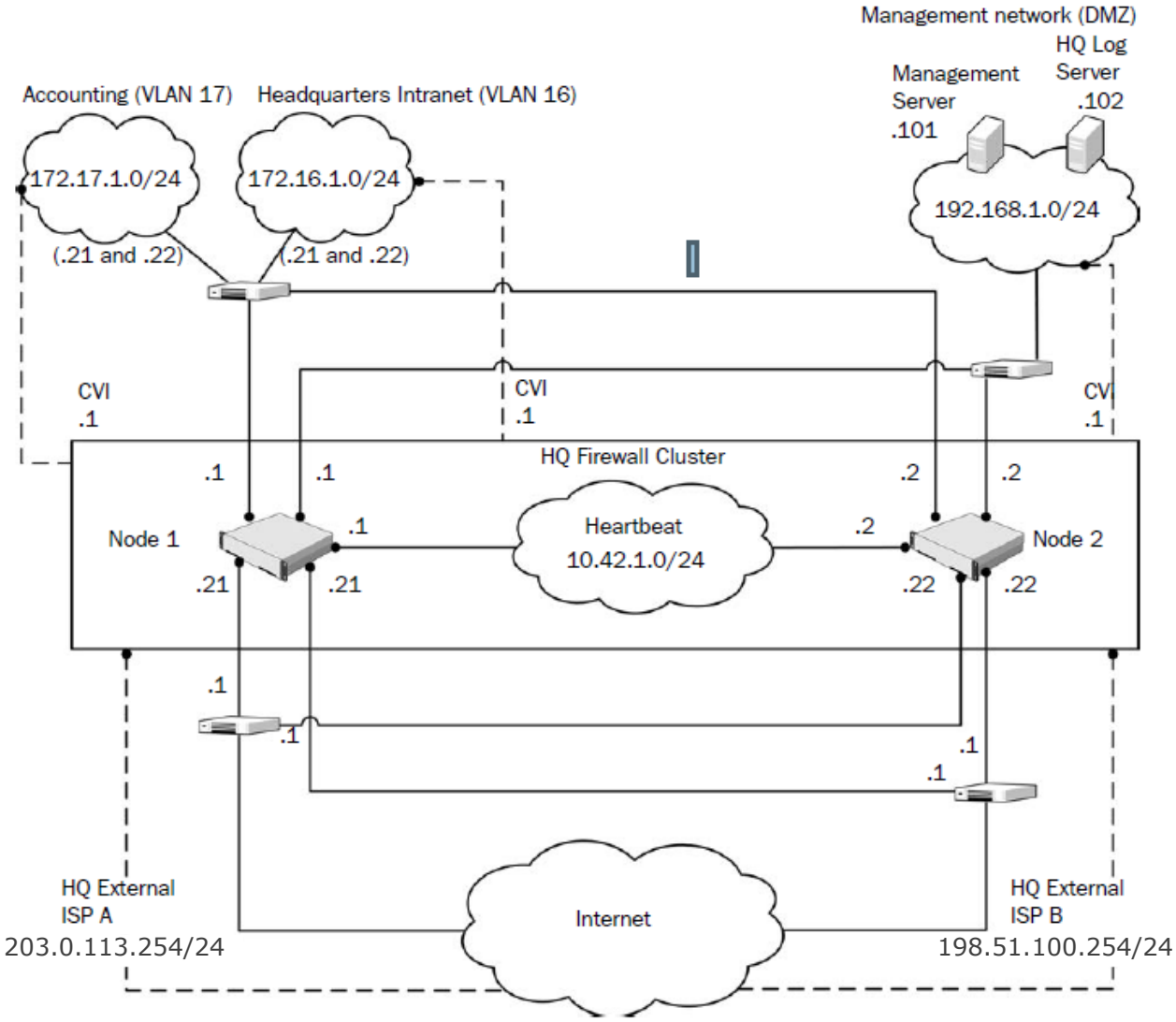
The example outlines a network with two firewalls: a Single Firewall at a branch office and a Firewall Cluster at headquarters.

Example Firewall Cluster

This example shows Firewall Cluster interfaces in the example network.

In the example network, the HQ Firewall Cluster is located in the Headquarters network. The cluster consists of two cluster nodes: Node 1 and Node 2.

Example firewall scenario



Network	Description
Heartbeat network	The heartbeat and cluster synchronization goes through the heartbeat network. CVI: no CVI defined. NDI: 10.42.1.1 (Node 1) and 10.42.1.2 (Node 2).
Management network (DMZ)	The management network interface is used for the control connections from the Management Server and for connecting to the HQ Log Server. CVI: 192.168.10.1. NDI: 192.168.10.21 (Node 1) and 192.168.10.22 (Node 2).

Network	Description
ISP A external network	This connection is one of the 2 Internet connections from the Headquarters site. It is provided by ISP A. CVI: 203.0.113.254. NDI: 203.0.113.21 (Node 1) and 203.0.113.22 (Node 2). Next-hop router: 203.0.113.1.
ISP B external network	This connection is the other of the 2 Internet connections from the Headquarters site. It is provided by ISP B. CVI: 198.51.100.254. NDI: 198.51.100.21 (Node 1) and 198.51.100.22 (Node 2). Next-hop router: 198.51.100.1.
HQ intranet	This VLAN (VLAN ID 16) is connected to the same network interface on the firewall with the HQ Accounting VLAN. CVI: 172.16.1.1. NDI: 172.16.1.21 (Node 1) and 172.16.1.22 (Node 2).
HQ Accounting network	This VLAN (VLAN ID 17) is connected to the same network interface on the firewall with the HQ intranet VLAN. CVI: 172.17.1.1. NDI: 172.17.1.21 (Node 1) and 172.17.1.22 (Node 2).

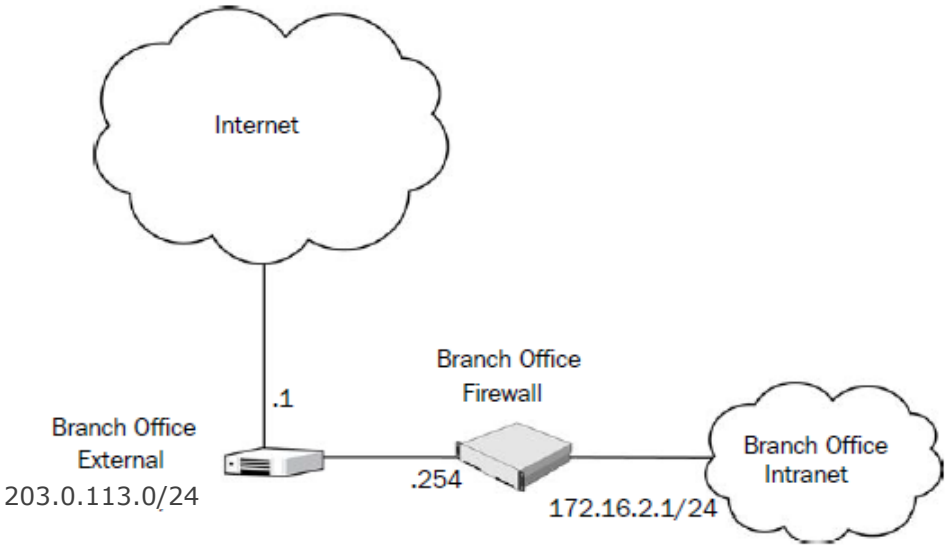
The Management Server and the HQ Log Server are at the headquarters site, in the DMZ network.

Security Management Center (SMC) component	Description
Management Server	This Management Server manages all firewalls and Log Servers of the example network. The Management Server in the Headquarters' Management Network (DMZ) with the IP address 192.168.1.101.
HQ Log Server	This Log Server receives log data from the firewalls. The server is located in the Headquarters' Management Network (DMZ) with the IP address 192.168.1.102.

Example Single Firewall

The Branch Office firewall is a Single Firewall located in the Branch Office network.

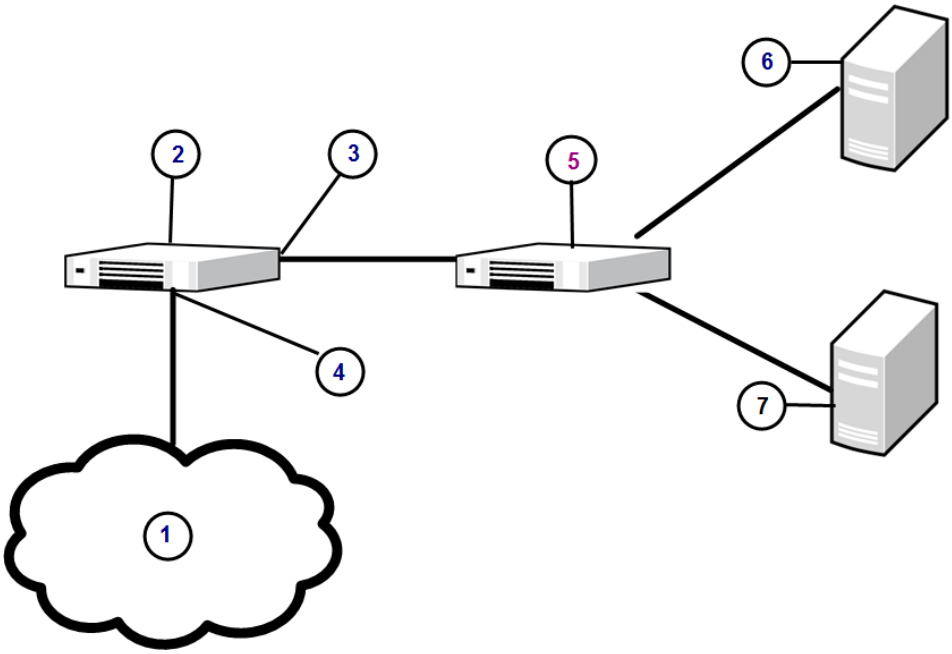
Example Single Firewall



Example headquarters management network

This example shows a sample management network.

Example HQ management network



1. Internet
2. HQ firewall
3. 192.168.10.1
4. 203.0.113.254
5. Switch
6. Management Server 192.168.10.200
7. HQ Log Server 192.168.10.201

HQ firewall

The HQ firewall provides NAT for the headquarters management network.

The HQ Firewall uses the following IP addresses with the headquarters management network:

- Internal: 192.168.10.1
- External: 203.0.113.254

SMC Servers

The example network includes a Management Server and a Log Server.

The following SMC Servers are included in the example network.

SMC Server	Description
Management Server	The Management Server is located in the headquarters' management network with the IP address 192.168.10.200. This Management Server manages all IPS engines, Firewalls, and Log Servers of the example network.
HQ Log Server	This server is located in the headquarters' management network with the IP address 192.168.10.201. This Log Server receives alerts, log data, and event data from the DMZ IPS and from the HQ IPS Cluster

Appendix G

Example network (IPS)

Contents

To give you a better understanding of how Forcepoint NGFW in the IPS role fits into a network, this example outlines a network with IPS engines.

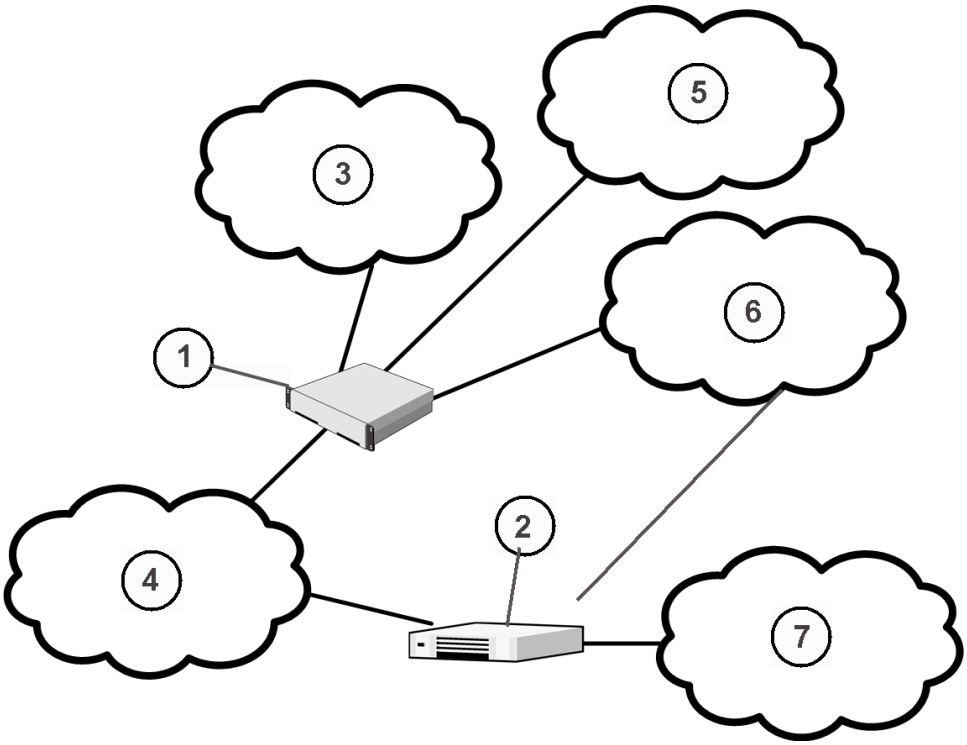
Example network overview (IPS)

This example network environment is used in all IPS examples.

There are two example IPS installations:

- An IPS Cluster in the Headquarters intranet network.
- A Single IPS in the Headquarters DMZ network.

Example network

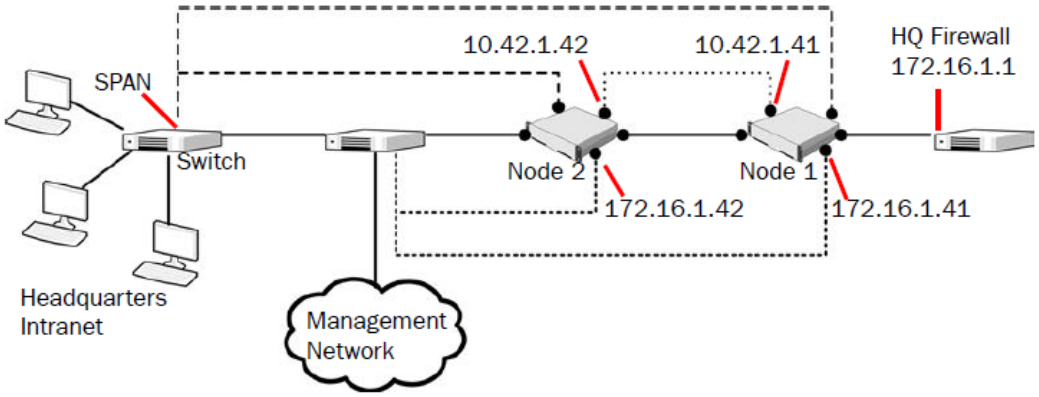


1	HQ firewall
2	Branch office firewall
3	HQ DMZ 192.168.1.0/24
4	Internet
5	HQ intranet 172.16.1.0/24
6	HQ Management 192.168.10.0/24
7	Branch Office intranet 172.16.1.0/24

Example headquarters intranet network

This example shows a sample headquarters intranet network.

Example headquarters intranet network.



HQ IPS Cluster

In this example, the HQ IPS Cluster is an inline serial cluster located in the Headquarters network.

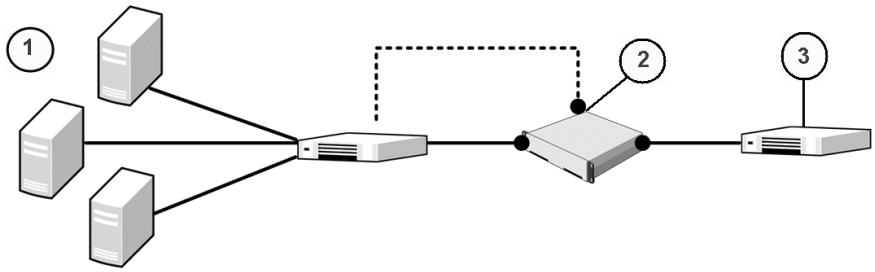
The cluster consists of two IPS engine nodes: Node 1 and Node 2.

Network interface	Description
Capture Interfaces	The HQ IPS Cluster's capture interface on each node is connected to a SPAN port in the headquarters intranet switch. All traffic in this network segment is forwarded to the SPAN ports for inspection.
Inline Interfaces	The cluster is deployed in the path of traffic between the firewall and the headquarters intranet switch. All traffic flows through each node's Inline Interface pair.
Normal Interfaces	The normal interface on each node is connected to the headquarters intranet switch. Node 1's IP address is 172.16.1.41 and Node 2's address is 172.16.1.42. This normal interface is used for control connections from the Management Server, sending events to the HQ Log Server, and for sending TCP resets
Heartbeat Interfaces	The nodes have dedicated Heartbeat Interfaces. Node 1 uses the IP address 10.42.1.41 and Node 2 uses the IP address 10.42.1.42.

Example headquarters DMZ network

This example shows a sample DMZ network.

Example headquarters DMZ network



1. DMZ servers
2. 192.168.1.41
3. HQ Firewall 192.168.1.1

DMZ IPS

In this example, the DMZ IPS in the headquarters DMZ network is a single inline IPS engine.

Network interface	Description
Inline Interfaces	The DMZ IPS is deployed in the path of traffic between the firewall and the DMZ network switch. All traffic flows through the IPS engine's inline interface pair.
Normal Interfaces	The normal interface is connected to the DMZ network using the IP address 192.168.1.41. This normal interface is used for control connections from the Management Server, sending event information to the HQ Log Server, and for TCP connection termination.

Appendix H

Cluster installation worksheet instructions

Contents

For planning the configuration of network interfaces for the engine nodes, use the worksheet.

- **Interface ID** — Write the Interface ID (and the VLAN ID, if VLAN tagging is used).
- **CVI** — Write the Interface ID's CVI information (if any) and on the **NDI** line, write the interfaces NDI information (if any). Use multiple lines for an Interface ID if it has multiple CVIs/NDIs defined.
- **Mode** — Select all modes that apply for this Interface ID.
- **IP Address** and **Netmask** — Define the CVI or NDI network address.
- **MAC/IGMP IP Address** — Define the MAC address used. If the interface's CVI Mode is Multicast with IGMP, define the multicast IP address used for generating automatically the multicast MAC address.
- **Comments** — Define, for example, a name of the connected network. Show how the NDI addresses differ between the nodes. Define a management interface's contact address if different from the interface's IP address.

Interface modes are explained in the following table. These same character codes are displayed in the firewall element interface properties of the Management Client.

Cluster installation worksheet

The following modes apply in the worksheet.

- **CVI mode** — U=Unicast MAC, M=Multicast MAC, I=Multicast with IGMP, K=Packet Dispatch, A=Interface's IP address used as the identity for authentication requests
- **NDI modes** — H=Primary heartbeat, h=Backup heartbeat, C=Primary control IP address, c=Backup control IP address, D=Default IP address for outgoing connection

Interface ID	Type	Mode	IP Address	Netmask	MAC / IGMP IP Address
	CVI	U M I K A	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: ___ . ___ . ___ . ___
	NDI	H h C c D	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___
	Comments				
	CVI	U M I K A	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: ___ . ___ . ___ . ___

Interface ID	Type	Mode	IP Address	Netmask	MAC / IGMP IP Address
	NDI	H h C c D	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___
	Comments				
	CVI	U M I K A	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: ___ . ___ . ___ . ___
	NDI	H h C c D	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___
	Comments				
	CVI	U M I K A	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: ___ . ___ . ___ . ___
	NDI	H h C c D	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___
	Comments				
	CVI	U M I K A	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: ___ . ___ . ___ . ___
	NDI	H h C c D	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___
	Comments				
	CVI	U M I K A	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: ___ . ___ . ___ . ___
	NDI	H h C c D	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___
	Comments				
	CVI	U M I K A	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___ or IGMP IP: ___ . ___ . ___ . ___
	NDI	H h C c D	___ . ___ . ___ . ___	___ . ___ . ___ . ___	MAC: ___ : ___ : ___ : ___ : ___ : ___
	Comments				