



FORCEPOINT

Next Generation Firewall

**Common Criteria Evaluated
Configuration Guide**

6.5.4

Revision D

Contents

- [Introduction](#) on page 2
- [Evaluated capabilities](#) on page 3
- [How firewalls process traffic](#) on page 4
- [Establishing a security configuration](#) on page 6
- [Secure the update process](#) on page 47
- [Network processes](#) on page 48

Introduction

This guide describes the requirements and guidelines for configuring the Forcepoint Next Generation Firewall (Forcepoint NGFW) system to comply with Common Criteria evaluation standards.

The system includes:

- Centralized management hardware on the Forcepoint NGFW Security Management Center Appliance (SMC Appliance) with a pre-installed Management Server and Log Server
- One or more Forcepoint NGFW Engines in the Firewall/VPN role that run on pre-installed NGFW appliances.

Evaluated products

The identification for the evaluated product is Forcepoint NGFW 6.5.

The target of evaluation consists of:




- Forcepoint NGFW Security Management Center (SMC) Appliance running software version 6.5.7 with:
 - OpenSSL FIPS Object Module SE #2398 version 2.0.13
 - Bouncy Castle FIPS Java API #3514 version 1.0.2 JCA/JCE provider
- Forcepoint NGFW Engine running software version 6.5.4 with:
 - OpenSSL FIPS Object Module SE #2398 version 2.0.14
 - Forcepoint NGFW Cryptographic Library #2319
 - Desktop appliance models: 330, 335
 - 1U appliance models: 1101, 1105, 2101, 2105
 - 2U appliance modes: 3301, 3305
 - 4U appliance model: 6205
 - Forcepoint NGFW Engine as a virtual machine on an ESXi server



Note: Cryptographic modules other than OpenSSL FIPS Object Module SE #2398 version 2.0.13, Bouncy Castle FIPS Java API #3514 version 1.0.2 JCA/JCE provider, Forcepoint NGFW Cryptographic Library #2319, and OpenSSL FIPS Object Module SE #2398 version 2.0.14, have not been evaluated nor tested during this Common Criteria evaluation.

Supporting documentation

These Forcepoint NGFW documents are referenced throughout this guide.

- *Forcepoint Next Generation Firewall Product Guide* , version 6.5, revision A
- *Forcepoint Next Generation Firewall Installation Guide* , version 6.5, revision A
- *How to install Forcepoint NGFW in FIPS mode* , version 6.5, revision A

Follow these steps to download the guides.

- 1) Go to <https://support.forcepoint.com/Documentation>.
- 2) Click **All Documents**.
- 3) Scroll down to **NETWORK SECURITY**, then under **Next Generation Firewall (NGFW)**, click **6.5**.

Evaluated capabilities

The Forcepoint NGFW system is comprised of several components that have specific capabilities that have been evaluated.


The following features have been evaluated in the product:

- Secure management functionality
- Stateful packet filtering firewall capabilities using Ethernet interfaces

Forcepoint NGFW system

The Forcepoint NGFW system combines centralized management and firewalls into one platform.

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

Component	Description
Management Client	<p>The Management Client is the user interface for the SMC. The Management Client version must match the version of the SMC.</p> <div>  <p>Note: The Management Client is used to configure the Management Server and Log Server, but the Management Client itself is not part of the target of evaluation.</p> </div> <p>You use the Management Client for all configuration and monitoring tasks. This interface allows the administrator to configure, monitor, and create reports about the whole Forcepoint NGFW system with the same tools and within the same user session.</p> <ul style="list-style-type: none"> • You can install the Management Client locally as an application, or you can start the Management Client with a web browser using the Java Web Start feature. • You can install an unlimited number of Management Clients. • Multiple administrators can log on at the same time to efficiently configure and monitor all NGFW Engines.

Component	Description
SMC servers	<p>SMC Appliance provides a unified hardware appliance that includes a dedicated Management Server and Log Server. All upgrades and patches, including operating system updates, come from Forcepoint.</p> <p>The Management Server stores an audit trail of administrator actions. The Management Server and Log Server can be configured to forward all audit information to an external audit server.</p>
Forcepoint NGFW Engines	<p>NGFW Engines inspect network traffic. They include an integrated operating system (a specially hardened version of Linux). There is no need for separate operating system patches or upgrades because all the software on the NGFW Engines is upgraded during the software upgrade. The Firewall policies determine when to use stateful connection tracking, packet filtering, or application-level security.</p>

Benefits of SMC management

SMC offers centralized remote management of system components and support for large-scale installations.

A centralized point for managing all system components simplifies the system administration significantly. Ease of administration is central to the SMC. The centralized management system:

- Provides administrators with visibility into the whole network.
- Simplifies and automates system maintenance tasks.
- Reduces the work required to configure the system.
- You can also combine information from different sources without having to integrate the components with an external system.

The main centralized management features include:

- Sharing configuration data in different configurations eliminates the need for duplicate work, which reduces the complexity of configurations and the amount of work required for changes. For example, an IP address used in the configurations of several different NGFW Engines has to be changed only one time in one place. It has to be changed only once because it is defined as a reusable element in the system.
- Remote upgrades can be downloaded and pushed automatically to several components. One remote upgrade operation updates all necessary details about the NGFW Engines, including operating system patches and updates.
- Fail-safe policy installation with automatic rollback to prevent policies that prevent management connections from being installed.
- The integrated backup feature allows saving all system configurations stored on the Management Server in one manually or automatically run backup.
- Central access point for administrators with centralized access control. Several administrators can be logged on at the same time and simultaneously change the system. Conflicting changes are automatically prevented. Administrator rights can be easily adjusted in a highly granular way.

How firewalls process traffic

NGFW Engines permit or deny traffic according to firewall filtering rules that are contained in a Firewall Policy.

Each policy is based on a Template Policy. A Template Policy contains necessary predefined rules and also enables automatic rules for the NGFW Engine to communicate with the SMC. A firewall only passes the traffic that is explicitly allowed in the Firewall Policy.

Access rules are traffic handling rules that define how the traffic is examined and what action the NGFW Engine takes when a rule is matched. You can use the Source, Destination, and Service options to set the matching criteria for the rule. For more information, see the *Configuring Access rules* topic in the *Access rules* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

Network packets are accepted automatically without additional processing when connection tracking is enabled. When Strict connection tracking mode is used, the NGFW Engine checks the sequence numbers of the packets in pre-connection establishment states and for RST and FIN packets, and drops packets that are out of sequence. Connections are closed upon completion of the flow (in the case of TCP and FTP) or if there is an inactivity timeout for the session.

Forcepoint NGFW supports several protocols and their attributes in a firewall policy. The protocols listed in the table are supported. Within each protocol, certain attributes are subject to firewall filtering rules.

Protocol	Attributes used for matching
RFC 792 (ICMPv4)	<ul style="list-style-type: none"> Type Code
RFC 4443 (ICMPv6)	<ul style="list-style-type: none"> Type Code
RFC 791 (IPv4)	<ul style="list-style-type: none"> Source address Destination address Transport layer protocol
RFC 2460 (IPv6)	<ul style="list-style-type: none"> Source address Destination address Transport layer protocol
RFC 793 (TCP)	<ul style="list-style-type: none"> Source port Destination port
RFC 768 (UDP)	<ul style="list-style-type: none"> Source port Destination port



Note: With stateful connections, a log entry is created only for the first packet that is seen in the control connection or data connection.



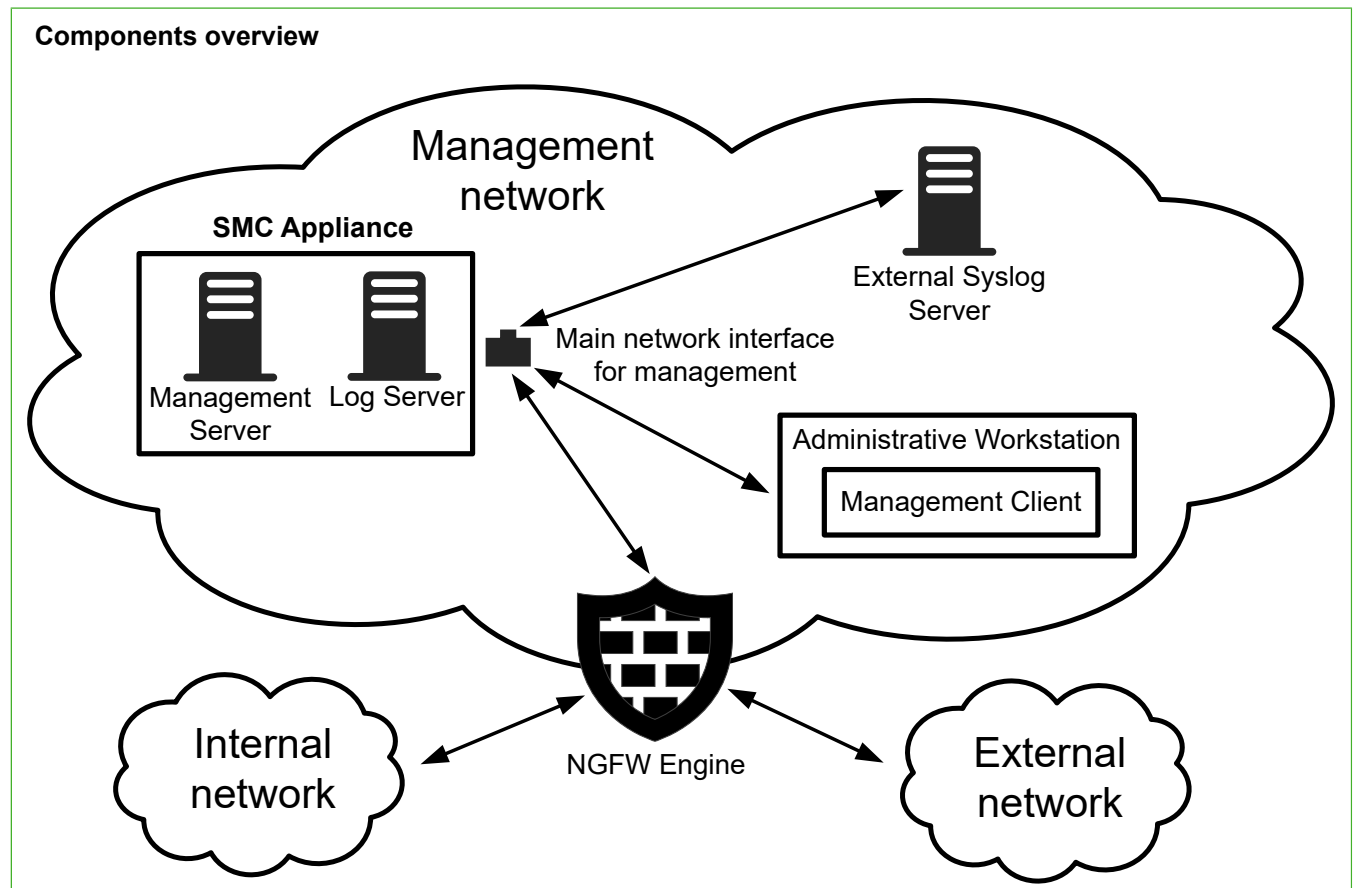
Note: TCP traffic on port 21 is by default interpreted as FTP protocol (RFC 959) traffic. If this control connection is allowed by Access rules and traffic on port 21 contains valid FTP protocol commands to open a data connection, the NGFW Engine allows those related data connections and logs them using the same settings as configured in Access rules for control connections.

For more information on the FTP Protocol Agent, see the *Define FTP Protocol parameters* topic in the *Working with Service elements* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

For more information on dynamic session establishment capabilities, see the *Support for multi-layer inspection* topic in the *Introduction to Forcepoint NGFW in the Firewall/VPN role* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

Establishing a security configuration

A Common Criteria configuration requires a specific configuration of the SMC Appliance, SMC software, and NGFW Engines.



These high-level steps are an overview of the process to configure the SMC Appliance and NGFW appliances for the Common Criteria evaluated configuration.

- 1) Enable FIPS mode at the SMC Appliance startup. The SMC Appliance runs a series of self-tests.
- 2) If the SMC Appliance self-tests result in errors, reset the appliance to factory settings.
- 3) Install the Management Client, then configure the security parameters for the Common Criteria evaluated configuration.
- 4) Create and install NGFW Engines in FIPS mode. The NGFW appliance runs a series of self-tests.
- 5) If the NGFW appliance self-tests result in errors, reset the appliance to factory settings.
- 6) Review the audit events.

FIPS mode restrictions

When FIPS mode is enabled, example restrictions are:

- The NGFW Engine local console, command line interface, and SSH access are not available
- The available cryptographic algorithms and configuration options in the SMC are restricted:
 - RSA key sizes of 2048 bits or greater are used for digital signature generation
 - ECDSA key sizes of 256 bits or greater are used for digital signature generation
 - SHA-1 cannot be used for digital signature generation

Enable FIPS mode on the SMC Appliance

To comply with Common Criteria evaluation standards, you must enable FIPS mode and enable 256-bit encryption as the security strength when you install the SMC Appliance.

Before you begin

Prepare the appliance for installation:

- Determine the appliance networking information:
 - IPv4 network address and network mask
 - (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 Remote Management Module port.

When 256-bit encryption is enabled, the SMC TLS Client and Server settings are automatically configured to use:

- TLS 1.2 as the protocol
- ECDSA P-521 certificates with SHA-512 in digital signatures
- P-521, P-384, and P-256 NIST curves in TLS key establishment

The Management Server and Log Server accept the following TLS cipher suites:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Use the main network interface for management for the connection to the NGFW Engine, and for the connection to the Management Client and external syslog server.

Set the time and date manually on the SMC Appliance. Although the product supports network time protocol (NTP), NTP is not to be used in the Common Criteria evaluated configuration.

For more information, see the topic *Installing the SMC Appliance in FIPS mode* in the document *How to install Forcepoint NGFW in FIPS mode*.

Related tasks

[Configure settings for an evaluated configuration](#) on page 8

Verify the SMC Appliance self-tests

The SMC Appliance contains several modules that run self-tests when the SMC Appliance starts.

For more information, see the topic *Check the SMC Appliance self-tests* in the document *How to install Forcepoint NGFW in FIPS mode*.

If a self-test fails, see the topic *Reset the SMC Appliance to factory settings* in the document *How to install Forcepoint NGFW in FIPS mode*.

Install the Management Client


If you are using the SMC Appliance or if you did not install the Management Client on the same computer as the Management Server, you must separately install the Management Client in FIPS mode.


For more information, see the topic *Install the Management Client in FIPS mode* in the document *How to install Forcepoint NGFW in FIPS mode*.


When logging on to the Management Client, the fingerprint of the Management Server certificate is verified. For more information, see the *Accept the Management Server certificate* topic in the *Installing the SMC* chapter in the *Forcepoint Next Generation Firewall Installation Guide*.

Configure settings for an evaluated configuration

After installing the SMC, several areas of the Management Client must be configured specifically for a Common Criteria evaluated configuration.

Setting	Configuration
Time Management	<p>To set the date and time manually on the SMC Appliance, enter:</p> <pre>sudo date -s '<YYYY-MM-DD hh:mm:ss>'</pre> <p>where <code><YYYY-MM-DD hh:mm:ss></code> is the date and time.</p> <div>  <p>Note: Although the product supports network time protocol (NTP), NTP is not to be used in the Common Criteria evaluated configuration.</p> </div>
Audit Server Configuration	<p>Follow the guidelines in the <i>Configuring the Log Server</i> chapter, the <i>Using certificates to secure communications to external components</i> topic in the <i>Managing certificates for system communications</i> chapter, and the <i>Forward audit data from Management Servers to external hosts</i> topic in the <i>Reconfiguring the SMC and engines</i> chapter in the <i>Forcepoint Next Generation Firewall Product Guide</i>.</p> <p>When setting the options for log or audit data forwarding in the properties of the Management Server or Log Server, select Use Internal Certificate or Use Imported Certificate as the TLS certificate to use.</p>
Audit Server Configuration (continued)	<p>1) Configure the trusted root CA certificate for the audit server.</p> <p>See the <i>Create Trusted Certificate Authority elements</i> topic in the <i>Managing certificates for system communications</i> chapter in the <i>Forcepoint Next Generation Firewall Product Guide</i></p>

Setting	Configuration
Audit Server Configuration (continued)	<p>2) If using an imported certificate, configure the trusted CA certificates for the client certificate.</p> <p>3) If using an imported certificate, generate the client certificate request.</p> <ul style="list-style-type: none"> See the <i>Create a certificate request</i> topic in the <i>Managing certificates for system communications</i> chapter in the <i>Forcepoint Next Generation Firewall Product Guide</i>. Select an RSA with the key size 2048 bits or greater, or ECDSA with 521 for P-521, 384 for P-384, or 256 for P-256 as the key size. The selected TLS cipher suite must match. <div>  <p>Note: After creating a certificate request, you must close and re-open the Management Client in order to export the certificate request.</p> </div>
Audit Server Configuration (continued)	<p>4) Configure the TLS profile using TLS 1.2.</p> <ul style="list-style-type: none"> The cipher suites that can be used: <ul style="list-style-type: none"> TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 When using an ECDHE cipher suite, P-521, P-384, and P-256 are automatically used in the TLS key establishment. Select the trusted CAs.
Audit Server Configuration (continued)	<p>5) Configure the server identity. Define the following settings for the TLS Server Identity:</p> <ul style="list-style-type: none"> TLS Server Identity — DNS Name Identity Value — the DNS name of the audit server. <p>For more information, see the <i>Configure TLS server identity</i> topic in the <i>Managing certificates for system communications</i> chapter in the <i>Forcepoint Next Generation Firewall Product Guide</i>.</p>

Setting	Configuration
Audit Server Configuration (continued)	<p>If the log or audit data forwarding connection to the audit server is not working, do the following:</p> <ul style="list-style-type: none"> In the properties of the Management Server, verify the settings on the Audit Forwarding tab. In the properties of the Log Server, verify the settings on the Log Forwarding tab. Restart the Management Server on the local console. Use the command: <code>sudo /etc/init.d/sgMgtServer restart</code> Restart the Log Server on the local console. Use the command: <code>sudo /etc/init.d/sgLogServer restart</code>
Logon Banner	<p>Follow the guidelines in the <i>Create logon banners for administrators</i> topic in the <i>Using the Management Client</i> chapter in the <i>Forcepoint Next Generation Firewall Product Guide</i>.</p>
Administrative Logins	<p>Follow the guidelines in the <i>Administrator accounts</i> chapter in the <i>Forcepoint Next Generation Firewall Product Guide</i>.</p> <p>Use the Management Client to manage users and passwords in the SMC. The local console user accounts are synchronized with the user accounts used in the SMC. The local console accounts and passwords are managed from the SMC. Only SMC user accounts with unrestricted permissions are available on the SMC Appliance local console.</p>
Administrative Logins (continued)	<p>To specify the timeout to terminate an inactive local administrative session, enter:</p> <pre>TMOUT=<TIMEOUT>;echo "export TMOUT=\$TMOUT" >> ~/.bashrc;logger -s -p local3.info "changed console timeout to \$TMOUT"</pre> <p>where <TIMEOUT> is the timeout in seconds.</p> <p>To enable temporarily locking administrator accounts after a certain amount of failed logon attempts:</p> <ol style="list-style-type: none"> In the Management Client, select Menu > System Tools > Global System Properties. On the Password Policy tab, select Enforce Password Settings for All the Administrators and Web Portal Users. In the Logon options section, select Temporarily Lock Account After Failed Logon Attempts. Enter the maximum number of failed logon attempts, and set how long to lock the account for. Click OK. <div>  <p>Note: If the administrator account is locked, it is still possible to log on to the SMC Appliance through the local console.</p> </div> <p>For information about setting timeouts in the Management Client and locking administrator accounts, see the <i>Enable and define password policy settings</i> topic in the <i>Administrator accounts</i> chapter in the <i>Forcepoint Next Generation Firewall Product Guide</i></p>

Setting	Configuration
Administrative Logins (continued)	<p>To manually log out of the local console account, enter:</p> <pre>logout</pre> <p>To log out of the Management Client, select Menu > File > Exit.</p>
Password Guidelines	<p>Follow the guidelines in the <i>Enable and define password policy settings</i> topic in the <i>Administrator accounts</i> chapter in the <i>Forcepoint Next Generation Firewall Product Guide</i>.</p> <p>When setting a password, you should select a password that meets these requirements:</p> <ul style="list-style-type: none"> • Minimum ten characters long • At least one uppercase character • At least one number • At least one special character: "!", "@", "#", "\$", "%", "^", "&", "*", "(", " ", ")" • Cannot be the same as the user name <p>By default, Forcepoint NGFW enforces a minimum password length of 10 characters. When operating in a Common Criteria evaluated configuration, we recommend that you set the minimum password length to 15 characters. Configure the Minimum Amount of Mandatory Characters setting to enforce these recommendations.</p>
Firewall Policy	<p>Use the Firewall Template Policy as the basis for creating a customized Firewall Template Policy and security policies that are compliant with Common Criteria. For more information, see the topics in this document about creating a customized Firewall Policy Template and creating a Firewall Policy. See also the <i>Creating and managing policy elements</i> chapter and the <i>Access rules</i> chapter in the <i>Forcepoint Next Generation Firewall Product Guide</i>.</p>

Create a Task to delete log and audit data

The NGFW Engine stores log data temporarily until the data is sent to the Log Server. The Management Server and Log Server store audit and log data locally, then send the data to an external audit server. Locally-stored data is not deleted automatically.


The behavior when remaining audit storage space starts to become low is as follows:

- **Log Server** — When the remaining audit storage space drops below 300MB, an alert is sent to administrators. When less than 100MB of space remains, the Log Server stops accepting new audit messages from NGFW Engines. The administrator has to take action to remove old audit records.
- **Management Server** — When less than 100MB of audit storage space remains, the Management Server prevents the administrator from making further changes. The administrator has to take action to remove old audit records.

When the **Log Spooling Policy** option is **Stop Traffic**, the NGFW Engine goes offline when the local storage space is full. This can happen when the Log Server is not available or when the Log Server storage space is becoming full and the Log Server stops the log reception. To check what the **Log Spooling Policy** option is set to for an NGFW Engine, in the Engine Editor, browse to **Advanced Settings > Log handling**.

For more information, see the *Managing and scheduling Tasks* chapter in 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**, then browse to **Administration**.
- 2) Browse to **Tasks**.
- 3) Right-click **Tasks**, then select **New > Delete Log Task**.
- 4) Select the Management Server and Log Server, then click **Add**.
- 5) On the **Task** tab, under **Target Data**, select all the log data types.
- 6) Under **Time Range**, select **Before**, and under **Log Server time**, select **Before 12 Months ago**, for example.
- 7) Click **OK**.
- 8) Browse to **Definition**.
- 9) Right-click the Task that you created, then select **Start** or **Schedule**.

Create an element for the NGFW Engine

Use the Management Client to create the NGFW Engine element.

These steps are the high-level tasks. For more information, see the *Creating and modifying engine elements* chapter in 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) In the Management Client, create an NGFW Engine, then define the properties in the Engine Editor. Follow the normal process to define the properties of an NGFW Engine, with these exceptions:
 - On the **Advanced Settings** branch, select **FIPS-Compatible Operating Mode**.
 - On the **Advanced Settings > Traffic Handling** branch, for **Layer 3 Connection Tracking Mode**, select **Strict**.
 - On the **Advanced Settings > Log Handling** branch, for **Log Spooling Policy**, select **Stop Traffic**.
 - On the **Advanced Settings > DoS Protection** branch, set **Rate-Based DoS Protection Mode** to **On**, then set a value for the **Limit for Half-Open TCP Connections** option. The limit applies per destination IP address. This option is enabled for all permitted traffic on the NGFW Engine, but can be overridden for some traffic in the Access rule options in a Firewall Policy.

Create a customized Firewall Policy Template

For a Common Criteria installation, add specific Access rules to a customized Firewall Policy Template, then use that template to create security policies.

These steps are the high-level tasks. For more information, see the *Creating and managing policy elements* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

Packet validity checks automatically drop invalid IP packets, packets with certain IP options, incomplete IP packets, and invalid IP fragments. These dropped packets are also logged when Packet Filter diagnostics have been enabled. The automatic anti-spoofing drops and logs spoofed packets where the source or the destination address is a loopback address, the source address is an IPv4 broadcast address or an IPv4 multicast address, or the source address does not belong to a connected network. The additional Access rules in the customized template discard IPv4 and IPv6 link local addresses, IPv6 reserved addresses, IPv4 and IPv6 addresses reserved for future use, and packets where the source address is an IPv6 multicast address.

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

1) Open the Firewall Policy Template for editing, then save it as Firewall cPP Template.

2) Create the following Network elements:

- For IPv4
 - The "IPv4 Link Local" network as 169.254.0.0/16.
 - The "IPv4 Reserved for Future Use" network as 240.0.0.0/4.
- For IPv6
 - The IPv6 networks 2d00:0000::/8, 2e00:0000::/7, and 3000:0000::/4 for RFC 3513 reserved addresses.
 - The Group element "RFC 3513 reserved addresses" that contains the networks above.
 - The IPv6 network "RFC 3513 Global Unicast Addresses" as 2000::/3.
 - The Expression element "IPv6 RFC 3513 reserved for future definition and use"

(negation of a union):

```
~ ( "RFC 3513 Global Unicast Addresses"
  U "IPv6 Unspecified Address"
  U "Localhost"
  U "IPv6 Multicast Network"
  U "Link-Local IPv6 Unicast Addresses" )
```

3) To add an Access rule, right-click the IPv4 Insert Point or IPv6 Insert Point, then select **Add Rule**.



Tip: You can right-click the ID cell to add more Access rules and to move Access rules up and down in the Policy.

4) To fill in the cell values for an Access rule, you can do the following:

- Drag elements to the cell from the resource pane on the left.
- Click the cell, then start typing to activate the look-ahead search.
- Double-click the cell to open a dialog box where you can configure the settings.

- 5) On the IPv4 Access tab, add the following rules to the beginning of the Access rules:

Source	Destination	Service	Action
IPv4 Link Local	ANY	ANY	Discard
ANY	IPv4 Link Local	ANY	Discard
IPv4 Reserved for Future Use	ANY	ANY	Discard
ANY	IPv4 Reserved for Future Use	ANY	Discard

- 6) On the IPv4 Access tab, disable or delete the following rule:

Source	Destination	Service	Action
ANY	ANY	Dest. Unreachable (Fragmentation Needed)	Allow; Connection Tracking: Normal

- 7) On the IPv6 Access tab, add the following rules to the beginning of the Access rules:

Source	Destination	Service	Action
IPv6 RFC 3513 reserved address	ANY	ANY	Discard
ANY	IPv6 RFC 3513 reserved address	ANY	Discard
Link-Local IPv6 Unicast Addresses	ANY	ANY	Discard
ANY	Link-Local IPv6 Unicast Addresses	ANY	Discard
IPv6 Multicast Network	ANY	ANY	Discard
IPv6 RFC 3513 reserved for future definition and use	ANY	ANY	Discard
ANY	IPv6 RFC 3513 reserved for future definition and use	ANY	Discard

- 8) On the IPv6 Access tab, disable or delete the following rules:

Source	Destination	Service	Action
ANY	ANY	IPv6 Neighbor Advertisement, IPv6 Neighbor Solicitation, IPv6 Redirect, IPv6 Router Advertisement, IPv6 Router Solicitation	Allow; DoS Protection: off; Scan Detection: off
ANY	ANY	IPv6 Packet Too Big	Allow; Connection Tracking: Normal

- 9) To allow IPv6 Neighbor Discovery, add the rules below. "IPv6 Solicited-Node Multicast" is defined as FF02::0:0:0:0:1:FF00::/104.

Source	Destination	Service	Action
ANY	IPv6 Solicited-Node Multicast	IPv6 Neighbor Solicitation	Allow
\$\$ Local Cluster(NDI IPv6 addresses only)	ANY	IPv6 Neighbor Advertisement	Allow
ANY	\$\$ Local Cluster(NDI IPv6 addresses only)	IPv6 Neighbor Advertisement	Allow



Note: The IPv6 Neighbor Discovery Protocol can be adversely affected when link local IPv6 addresses are discarded as required in a Common Criteria configuration. To allow IPv6 Neighbor Solicitation and Neighbor Advertisement messages using IPv6 link local addresses, add the following rules before the IPv6 link local discard rules:

Source	Destination	Service	Action
Link-Local IPv6 Unicast Addresses	IPv6 Solicited-Node Multicast, Link-Local IPv6 Unicast Addresses	IPv6 Neighbor Solicitation	Allow
IPv6 RFC 3513 Global Unicast Addresses, Link-Local IPv6 Unicast Addresses	Link-Local IPv6 Unicast Addresses	IPv6 Neighbor Advertisement	Allow

Create a Firewall Policy

After creating the customized Firewall Policy Template, create a Firewall Policy based on the template.

For more information, see the *Considerations for designing Access rules* topic in the *Access rules* chapter and the *Creating and managing policy elements* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

Access rules affect all network interfaces, unless the source interface is specified. For more information on using Zone elements, see the *Using Zone elements for interface matching in Access rules* topic in the *Access rules* chapter in 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) Create a Firewall Policy that uses the Firewall cPP Template.
- 2) To add an Access rule, right-click the IPv4 Insert Point or IPv6 Insert Point, then select **Add Rule**.



Tip: You can right-click the ID cell to add more Access rules and to move Access rules up and down in the Policy.

- 3) To fill in the cell values for an Access rule, you can do the following:
 - Drag elements to the cell from the resource pane on the left.
 - Click the cell, then start typing to activate the look-ahead search.
 - Double-click the cell to open a dialog box where you can configure the settings.
- 4) To configure the logging for a rule, double-click the **Logging** cell, then configure the settings. Select **Override Settings Inherited from Continue Rule(s)**, then set the **Log Level** to **Essential**.



Note: Packets that are automatically rejected are not logged by default. To enable the logging of all packets, right-click the NGFW Engine, select **Options > Diagnostics**, then under **Packet Processing**, select **Packet Filtering**. Click **OK** to close the dialog box.

Enabling communication between the SMC and NGFW Engine


You must make initial contact between the NGFW Engine and the Management Server of the SMC.

After initial contact is made, subsequent TLS connections between the components are mutually authenticated. The reference identifiers in the SAN DNS field and the DN field for subsequent TLS client and server authentication are configured automatically during the registration.

Save the initial configuration in the Management Client

You must save the initial configuration for the NGFW Engine.

Steps

- 1) Select  **Configuration**.
- 2) Right-click the NGFW Engine, then select **Configuration > Save Initial Configuration**.
- 3) Next to the **Initial Security Policy** field, click **Select**, then select the Firewall Policy that you created. The policy is automatically installed on the NGFW Engine after initial contact is made.
- 4) Click **View Details**.

Make note of the one-time generated password, the Management Server address, and the SHA-512 certificate fingerprint. You need this information when installing the NGFW Engine.
- 5) Click **OK**.

Install the NGFW Engine in FIPS mode

To comply with Common Criteria evaluation standards, you must enable FIPS mode and enable 256-bit encryption as the security strength when you install the NGFW Engine.

Management connections are protected by 256-bit encryption. Both 256-bit and 128-bit encryption can be used for audit export.

For more information, see the topic *Installing the NGFW Engine in FIPS mode* in the document *How to install Forcepoint NGFW in FIPS mode*. See also the *Forcepoint Next Generation Firewall Installation Guide*.

If you want to manually enter the SHA-512 certificate fingerprint that was shown when you saved the initial configuration in the Management Client, select **Edit Fingerprint** on the **Prepare for Management Contact** page. If you do not enter the fingerprint, the certificate fingerprint is shown later for you to verify.

If the initial contact fails, restart the appliance, start the NGFW Configuration Wizard again, and verify the following:

- The one-time generated password is correct
- The Management Server IP address is correct
- The certificate fingerprint is correct
- 256-bit encryption is used for the connection to the Management Server

Verify the NGFW Engine self-tests

The NGFW Engine contains the OpenSSL FIPS Object Module. The module runs several self-tests when the Forcepoint NGFW appliance starts.

For more information, see the topic *Check the NGFW Engine self-tests* in the document *How to install Forcepoint NGFW in FIPS mode*.

Verify the installed version of the SMC, NGFW Engine, and SMC Appliance

You can verify the installed version of the SMC, NGFW Engine, and the SMC Appliance.

Verify the SMC version

You can verify the SMC version in the Management Client.


Steps

- 1) Select **≡ Menu > Help > About**.
The version is shown in the dialog box that opens.

Verify the NGFW Engine version

You can verify the NGFW Engine version in the Management Client.

Steps

- 1) Select  **Home**.
- 2) Select the NGFW Engine.
On the **General** tab of the **Info** pane, the NGFW Engine version is shown under the **Version** label.

Verify the SMC Appliance version

You can verify the SMC Appliance version and installed patch using the appliance maintenance and bug remediation (AMBR) patching utility on the local console.

Steps

- 1) On the local console, log on to the SMC Appliance.
- 2) Enter the following command:

```
ambr-query
```

The current version and installed patch are shown.



Disabling communication between the SMC and NGFW Engine

You can disable communication from the perspective of the SMC or NGFW Engine.

Disable in the SMC by deleting the NGFW Engine element

To disable communication from the SMC, delete the NGFW Engine element in the Management Client.

Steps


- 1) Select  **Configuration**.
- 2) Right-click the NGFW Engine element, then select **Delete**.
- 3) Click **Yes** to confirm the deletion.
If any other elements refer to the NGFW Engine element, delete the references before you continue.
- 4) Select  **Menu** > **View** > **Panels** > **Trash**.
- 5) Right-click the NGFW element, then select **Delete**.

- Click **Yes** to confirm the permanent deletion.

Disable by resetting the NGFW Engine in the Management Client

You can reset the NGFW Engine to factory settings from the Management Client.

Steps

- Select  **Configuration**.
- Right-click the NGFW Engine, then select **Commands > Reset to Factory Settings**.
- In the **Number of Overwrites** field, enter how many times you want the stored data on the file system to be overwritten.
- If you want the appliance to turn off after the factory reset has completed, select **Shut Down After Reset**.
- Click **OK**.
- When asked to confirm the command, click **Yes**.

Disable by resetting the NGFW Engine from the console

You can use the local console to reset the NGFW Engine to factory settings.

For details, see the topic *Reset the NGFW appliance to factory settings* in the document *How to install Forcepoint NGFW in FIPS mode*.

Review audit events

Review these examples of audit events and records that appear in Common Criteria evaluated configuration.

The record contents are shown in McAfee ESM format. To set the format to use, see the *Add rules for forwarding audit data from Management Servers* topic in the *Reconfiguring the SMC and engines* chapter in the *Forcepoint Next Generation Firewall Product Guide*. Some of the more common McAfee ESM fields are described in the following table.

Field	Description
Timestamp	Log entry creation time.
Nodeld	IP address of the engine or server that sent the log entry.
Facility	The firewall subsystem that created the log entry.
Compld	The identifier of the creator of the log entry.

Field	Description
InfoMsg	A description of the log event that further explains the entry.
SenderType	The type of engine or server that sent the log entry.
EventId	Event identifier, unique within one sender.
UserOriginator	Administrator who triggered the audit event.
ClientIpAddress	Address of the client that triggered the audit event.
Type	Log entry severity type.
TypeDescription	Type of action that triggered the audit entry.
Result	Result state after the audited event.
ObjectName	Elements being manipulated in the audit event.
SituationId	The identifier of the situation that triggered the log event.
Situation	Situation name.

FAU_GEN.1.1 a)	
Auditable event	Startup and shutdown of the audit functions
Startup of SMC Appliance	<pre> May 1 16:25:56 192.0.2.2 Timestamp="2019-05-01 16:25:56", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8374310612217364481", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.start", Result="Success", ObjectName="Audit function started" May 1 16:26:20 192.0.2.2 Timestamp="2019-05-01 16:26:20", NodeId="192.0.2.2", CompId="", SenderType="Log Server", EventId="8374412862503780353", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.start", Result="Success", ObjectName="Audit function started" </pre>

FAU_GEN.1.1 a)	
Shutdown of SMC Appliance	<pre>May 1 16:29:56 192.0.2.2 Timestamp="2019-05-01 16:29:56", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", SenderType="Log Server", EventId="8374412862503780393", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.stop", Result="Success", ObjectName="Audit function shutdown" May 1 16:30:04 192.0.2.2 Timestamp="2019-05-01 16:30:04", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8374310612217364555", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.stop", Result="Success", ObjectName="Audit function shutdown"</pre>
Startup of NGFW Engine	<pre>May 1 15:50:39 192.0.2.2 Timestamp="2019-05-01 15:50:39", LogId="11", NodeId="192.0.2.4", Facility="System Utilities", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="Auditing log start", ReceptionTime="2019-05-01 15:50:39", SenderType="Firewall", SituationId="78022", Situation="System_Engine-Log-Auditing-State", EventId="6529381412783521803"</pre>
Shutdown of NGFW Engine	<pre>May 1 15:48:23 192.0.2.2 Timestamp="2019-05-01 15:48:23", LogId="2526", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="Auditing log end", ReceptionTime="2019-05-01 15:50:39", SenderType="Firewall", SituationId="78022", Situation="System_Engine-Log-Auditing-State", EventId="6529380841552873950"</pre>
FAU_GEN.1.1 c)	
Auditable event	Administrative login and logout

FAU_GEN.1.1 c)	
Administrative login	<pre>May 1 20:20:18 192.0.2.2 Timestamp="2019-05-01 20:20:18", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login succeeded for user admin in domain Shared Domain", SenderType="Management Server", EventId="8376289638658081680", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.login", Result="Success", ObjectName="admin;Shared Domain"</pre>
Administrative logout	<pre>May 1 20:23:54 192.0.2.2 Timestamp="2019-05-01 20:23:54", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Logout succeeded for user admin.", SenderType="Management Server", EventId="8376289638658081722", UserOriginator="System", ClientIpAddress="10.21.200.145", TypeDescription="stonegate.admin.logout", Result="Success", ObjectName="admin"</pre>
Auditable event	Security related configuration changes
Firewall filtering rule change	<pre>May 1 20:33:14 192.0.2.2 Timestamp="2019-05-01 20:33:14", NodeId="192.0.2.2", RuleId="147.2", CompId="Management Server", InfoMsg="IPv4 Access Rule @147.2 has been modified.", SenderType="Management Server", EventId="8376289638658081825", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.update", Result="Success", ObjectName="High Security Policy"</pre>
Firewall security policy change	<pre>May 1 20:33:14 192.0.2.2 Timestamp="2019-05-01 20:33:14", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8376289638658081826", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.update", Result="Success", ObjectName="High Security Policy"</pre> <pre>May 1 20:33:19 192.0.2.2 Timestamp="2019-05-01 20:33:19", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8376289638658081829", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.policy.upload.start", Result="Success", ObjectName="High Security Policy;NGFW-FIPS"</pre>

FAU_GEN.1.1 c)	
Firewall security policy change (continued)	<pre> May 1 20:34:01 192.0.2.2 Timestamp="2019-05-01 20:34:01", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8376289638658081836", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.firewall.policy.upload", Result="Success", ObjectName="NGFW-FIPS;High Security Policy" May 1 20:34:01 192.0.2.2 Timestamp="2019-05-01 20:34:01", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8376289638658081837", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.policy.upload.end", Result="Success", ObjectName="High Security Policy;NGFW-FIPS" </pre>
Audit server configuration changes	<pre> May 1 20:27:32 192.0.2.2 Timestamp="2019-05-01 20:27:32", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A new log forward rule was created with Audit types to host Audit Server ext (port 2055).", SenderType="Management Server", EventId="8376289638658081768", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.log.forward.new", Result="Success", ObjectName="Management Server" May 1 20:28:49 192.0.2.2 Timestamp="2019-05-01 20:28:49", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A log forward rule was deleted.", SenderType="Management Server", EventId="8376289638658081785", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.log.forward.deleted", Result="Success", ObjectName="Management Server" </pre>

FAU_GEN.1.1 c)	
Modification of administrator accounts	<pre>May 1 20:46:30 192.0.2.2 Timestamp="2019-05-01 20:46:30", NodeId="192.0.2.2",CompId="Management Server", SenderType="Management Server", EventId="8376289638658081943", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="admin2"</pre> <pre>May 1 20:47:10 192.0.2.2 Timestamp="2019-05-01 20:47:10", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8376289638658081946", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.disabled", Result="Success", ObjectName="admin2"</pre> <pre>May 1 20:47:14 192.0.2.2 Timestamp="2019-05-01 20:47:14", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8376289638658081947", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.enabled", Result="Success", ObjectName="admin2"</pre>
Auditable event	Changes to time
Manual time change	<pre>May 1 21:24:58 192.0.2.2 Timestamp="2019-05-01 21:24:58", NodeId="127.0.0.1", Type="Notification",CompId="3", InfoMsg="May 1 21:24:58 smca-fips sudo: admin : TTY=ttyl ; PWD=/home/admin ; USER=root ; COMMAND=/bin/date -s 2019-05-01 21:22:00", ReceptionTime="2019-05-01 21:24:58", SenderType="Third Party Device", EventId="2401"</pre>
Logon banner change	<pre>May 1 20:51:17 192.0.2.2 Timestamp="2019-05-01 20:51:17", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Updated Global System Property logon_banner_text to SMC Appliance.UNAUTHORIZED USE PROHIBITED.", SenderType="Management Server", EventId="8376289638658081973", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.update", Result="Success", ObjectName="logon_banner_text"</pre>

FAU_GEN.1.1 c)	
Minimum password length	<pre>May 1 20:52:44 192.0.2.2 Timestamp="2019-05-01 20:52:44", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Updated Global System Property password_character_number_minimum to 14", SenderType="Management Server", EventId="8376289638658081983", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.update", Result="Success", ObjectName="password_character_number_minimum"</pre>
Remote session timeout change	<pre>May 1 20:55:58 192.0.2.2 Timestamp="2019-05-01 20:55:58", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Updated Global System Property lock_screen_setting to true", SenderType="Management Server", EventId="8376289638658082002", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.update", Result="Success", ObjectName="lock_screen_setting"</pre>
Auditable event	Generating / import of, changing, or deleting of cryptographic keys
Creation of a TLS private key (Configuration > Administration > Certificates > TLS Credentials > New TLS Credentials)	<pre>May 1 21:42:53 192.0.2.2 Timestamp="2019-05-01 21:42:53", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Cryptographic key generated", SenderType="Management Server", EventId="8376289638658082174", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.cryptographic_key.new", Result="Success", ObjectName="Audit TLS Key"</pre>
Certificate signing request	<pre>May 1 22:31:28 192.0.2.2 Timestamp="2019-05-01 22:31:28", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Credentials certificate signing request was exported. The fingerprint is 55:1E:FB:29:F9:4E:F8:AB:1F:A8:A8:FE:45:A8:9C:55:A1:F4:87:2C.", SenderType="Management Server", EventId="8436275003044921357", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.certificate.export", Result="Success", ObjectName="Audit TLS Key"</pre>
Import signed certificate	<pre>May 3 20:58:17 192.0.2.2 Timestamp="2019-05-03 20:58:17", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8376289638658089403", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.certificate.import", Result="Success", ObjectName="Audit CSR"</pre>

FAU_GEN.1.1 c)	
Deletion (from Trash)	<pre>May 1 22:23:49 192.0.2.2 Timestamp="2019-05-01 22:23:49", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8376289638658082307", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.cryptographic_key.deleted", Result="Success", ObjectName="Audit TLS Key"</pre>
Import of a trusted certificate authority (CA)	<pre>May 1 21:46:34 192.0.2.2 Timestamp="2019-05-01 21:46:34", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="tls_certificate_authority element has been created.", SenderType="Management Server", EventId="8376289638658082183", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="Audit Trusted CA"</pre> <pre>May 1 21:46:35 192.0.2.2 Timestamp="2019-05-01 21:46:35", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A local certificate key was imported into a Trusted Certificate Authority.", SenderType="Management Server", EventId="8436275003044921355", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.certificate.import", Result="Success",ObjectName="Audit Trusted CA"</pre>

FAU_GEN.1.1 c)	
Import of a private key and a certificate	<pre>May 1 21:56:52 192.0.2.2 Timestamp="2019-05-01 21:56:52", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8376289638658082214", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.certificate.import", Result="Success", ObjectName="Audit key pair"</pre> <pre>May 1 21:56:52 192.0.2.2 Timestamp="2019-05-01 21:56:52", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Cryptographic key imported", SenderType="Management Server", EventId="8376289638658082215", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.cryptographic_key.import", Result="Success", ObjectName="Audit key pair"</pre> <pre>May 1 21:56:52 192.0.2.2 Timestamp="2019-05-01 21:56:52", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8376289638658082216", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="Audit key pair"</pre>
Auditable event	Resetting passwords
Password reset	<pre>May 1 21:13:45 192.0.2.2 Timestamp="2019-05-01 21:13:45", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8376289638658082060", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.password.change", Result="Success", ObjectName="admin2"</pre>
FAU_STG_EXT.1.3	
Auditable event	Action in case of possible audit data loss

FAU_STG_EXT.1.3

Using "Overwrite Oldest" setting when disk is full

```
May 22 17:57:59 10.116.240.254 Timestamp="2019-05-22 17:57:59",
NodeId="10.118.58.102",
CompId="LogServer 10.118.58.102",
InfoMsg="Some files must be deleted in order to free disk space for storage
files.",S
enderType="Log Server",
SituationId="512",
Situation="Log Server: disk full",
AlertSeverity="Critical",
EventId="1558547879977"
```

```
May 22 17:58:29 10.116.240.254 Timestamp="2019-05-22 17:58:29",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="May 22 17:58:29 smc-appliance-2 audispd: node=smc-appliance-2
type=PATH msg=audit(1558547909.679:96464): item=0
name='/usr/local/forcepoint/smc/data/storage/Firewall/
year2019/month05/day21/hour20/' inode=7077893 dev=fd:0a
mode=040755 ouid=499 ogid=500 rdev=00:00 obj=system_u:object_r:usr_t:s0
nametype=PARENT",
ReceptionTime="2019-05-22 17:58:29",
SenderType="Third Party Device",
EventId="486226"
```

```
May 22 17:58:29 10.116.240.254 Timestamp="2019-05-22 17:58:29",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="May 22 17:58:29 smc-appliance-2 audispd: node=smc-appliance-2
type=PATH msg=audit(1558547909.679:96464): item=1
name='/usr/local/forcepoint/smc/data/storage/Firewall/
year2019/month05/day21/hour20/
20190521_20_C0_169.254.253.253_0522154444875.arch' inode=7077894
dev=fd:0a mode=0100644 ouid=499 ogid=500 rdev=00:00
obj=system_u:object_r:usr_t:s0 nametype=DELETE",
ReceptionTime="2019-05-22 17:58:29",
SenderType="Third Party Device",
EventId="486227"
```

FCS_TLSC_EXT.1, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

Auditable event

TLS sessions

Failure of the trusted path functions

```
Aug 2 15:24:42 192.0.2.2 Timestamp="2019-08-02 15:24:42",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="TLS Connection failed : Protocol = NONE
Peer = [host=192.0.2.4
port=60688]
Local = [port=3021]
- Client requested protocol TLSv1.1 not enabled or not supported",
SenderType="Management Server",
EventId="7766082894518302730",
UserOriginator="System",
ClientIpAddress="192.0.2.4",
TypeDescription="stonegate.trusted.connection.failure",
Result="Fail"
```

FCS_TLSC_EXT.1, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2	
Failure to establish a TLS client session	<pre>May 2 22:14:22 192.0.2.2 Timestamp="2019-05-02 22:14:22", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.10 port=6514] Local = [host=192.0.2.2 port=48734] - Syslog authentication failed. [/192.0.2.10:6514] Details: Received fatal alert: handshake_failure", SenderType="Management Server", EventId="8376289638658087892", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>
Failure to establish a TLS server session	<pre>May 7 13:51:15 192.0.2.2 Timestamp="2019-05-07 13:51:15", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.11 port=35996] Local = [port=8905] - Client requested protocol TLSv1.1 not enabled or not supported", SenderType="Management Server", EventId="8376289638658111379", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>
FFW_RUL_EXT.1	
Auditable event	Indication of packets dropped due to too much network traffic
Indication of packets dropped due to too much network traffic	<pre>May 30 18:51:20 10.116.240.254 Timestamp="2019-05-30 18:51:20", LogId="2041025", NodeId="10.116.253.4", Facility="System Utilities", Type="Notification", Srcif="2", CompId="NGFW-335 node 1", ReceptionTime="2019-05-30 18:51:21", SenderType="Firewall", SituationId="78023", Situation="System_Engine-NIC-Dropped-RX-Packets", EventId="6539936131706725569"</pre>
Half-open connection limit	<pre>May 15 22:08:20 192.0.2.2 Timestamp="2019-05-15 22:08:20", LogId="10265652", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Dst="203.0.113.6", CompId="NGFW-FIPS node 1", InfoMsg="Protection started Trigger: half-open limit", ReceptionTime="2019-05-15 22:08:20", SenderType="Firewall", SituationId="79990", Situation="DOS_SYN-Flood-Started", EventId="6534549890528182469"</pre>

FFW_RUL_EXT.2	
Auditable event	Application of rules configured with the 'log' operation
Permitted traffic	<pre> Jul 24 16:11:30 192.0.2.2 Timestamp="2019-07-24 16:11:30", LogId="10275205", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="New connection", Action="Allow", Protocol="6", Src="198.51.100.6", Dst="203.0.113.6", Sport="36042", Dport="21", RuleId="105.1", Srcif="1", CompId="NGFW-FIPS node 1", ReceptionTime="2019-07-24 16:11:30", SenderType="Firewall", SituationId="70018", Situation="Connection Allowed", EventId="6559827237648990477", Service="FTP" </pre>
Denied traffic	<pre> Jul 24 16:16:51 192.0.2.2 Timestamp="2019-07-24 16:16:51", LogId="10275282", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="Connection discarded", Action="Discard", Protocol="6", Src="198.51.100.6", Dst="203.0.113.6", Sport="36044", Dport="21", RuleId="2097158.0", Srcif="1", CompId="NGFW-FIPS node 1", ReceptionTime="2019-07-24 16:16:51", SenderType="Firewall", SituationId="70019", Situation="Connection Discarded", EventId="6559828586268721427", Service="FTP" </pre>
FIA_AFL.1	
Auditable event	Unsuccessful login attempt limit is met or exceeded
Prevent the offending remote Administrator from successfully authenticating until an Administrator defined time period has elapsed	<pre> Jun 18 16:15:54 192.0.2.2 Timestamp="2019-06-18 16:15:54", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Delay after login failures. - Authentication failed. Username or password may be incorrect. Verify that address of the server is correct and that it is running properly. ", SenderType="Management Server", EventId="7377165990888473955", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="stonegate.admin.login", Result="Fail", ObjectName="admin1" </pre>

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Auditable event	All use of identification and authentication mechanism
Local session identification and authentication failures	<pre>May 2 22:30:47 192.0.2.2 Timestamp="2019-05-02 22:30:47",NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 2 22:30:47 smca-fips login: pam_unix(login:auth): check pass; user unknown", ReceptionTime="2019-05-02 22:30:47", SenderType="Third Party Device", EventId="3516"</pre> <pre>May 2 22:30:47 192.0.2.2 Timestamp="2019-05-02 22:30:47", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 2 22:30:47 smca-fips login: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=ttty1 ruser= rhost=", ReceptionTime="2019-05-02 22:30:47", SenderType="Third Party Device", EventId="3517"</pre>
Local session identification and authentication failures (continued)	<pre>May 2 22:30:47 192.0.2.2 Timestamp="2019-05-02 22:30:47", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 2 22:30:47 smca-fips login: pam_faillock(login:auth): User unknown", ReceptionTime="2019-05-02 22:30:47", SenderType="Third Party Device", EventId="3518"</pre> <pre>May 2 22:30:48 192.0.2.2 Timestamp="2019-05-02 22:30:48", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 2 22:30:48 smca-fips login: FAILED LOGIN SESSION FROM (null) FOR admin3 Permission denied", ReceptionTime="2019-05-02 22:30:48", SenderType="Third Party Device", EventId="3519"</pre>

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
<p>Local session identification and authentication failures (continued)</p>	<pre>May 2 22:36:08 192.0.2.2 Timestamp="2019-05-02 22:36:08", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 2 22:36:08 smca-fips unix_chkpwd[28271]: password check failed for user (admin)", ReceptionTime="2019-05-02 22:36:08", SenderType="Third Party Device", EventId="3533"</pre> <pre>May 2 22:36:08 192.0.2.2 Timestamp="2019-05-02 22:36:08", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 2 22:36:08 smca-fips login: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost= user=admin", ReceptionTime="2019-05-02 22:36:08", SenderType="Third Party Device", EventId="3534"</pre> <pre>May 2 22:36:10 192.0.2.2 Timestamp="2019-05-02 22:36:10", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 2 22:36:10 smca-fips login: FAILED LOGIN SESSION FROM (null) FOR admin Permission denied", ReceptionTime="2019-05-02 22:36:10", SenderType="Third Party Device", EventId="3535"</pre>
<p>Local session successful identification and authentication</p>	<pre>May 2 22:39:51 192.0.2.2 Timestamp="2019-05-02 22:39:51", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 2 22:39:51 smca-fips login: pam_unix(login:session): session opened for user admin by LOGIN(uid=0)", ReceptionTime="2019-05-02 22:39:51", SenderType="Third Party Device", EventId="3547"</pre> <pre>May 2 22:39:51 192.0.2.2 Timestamp="2019-05-02 22:39:51", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 2 22:39:51 smca-fips login: LOGIN ON tty1 BY admin", ReceptionTime="2019-05-02 22:39:51", SenderType="Third Party Device", EventId="3557"</pre>

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Remote session identification and authentication failures	<pre>May 2 22:44:15 192.0.2.2 Timestamp="2019-05-02 22:44:15", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login attempt for unknown user admin3", SenderType="Management Server", EventId="8376289638658088064", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.login", Result="Fail", ObjectName="Unknown user"</pre> <pre>May 2 22:44:15 192.0.2.2 Timestamp="2019-05-02 22:44:15", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login attempt for unknown user admin3. From 192.0.2.11.", SenderType="Management Server", SituationId="519", Situation="Management Server: Login failed", AlertSeverity="Low", EventId="1556837055770"</pre>
Remote session identification and authentication failures (continued)	<pre>May 2 23:00:25 192.0.2.2 Timestamp="2019-05-02 23:00:25", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="login failed for user admin. From 192.0.2.11.", SenderType="Management Server", SituationId="519", Situation="Management Server: Login failed", AlertSeverity="Low", EventId="1556838025764"</pre> <pre>May 2 23:00:25 192.0.2.2 Timestamp="2019-05-02 23:00:25", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login failed for user admin. - Authentication failed. Username or password may be incorrect. Verify that address of the server is correct and that it is running properly. ", SenderType="Management Server", EventId="8376289638658088122", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.login", Result="Fail", ObjectName="admin;Shared Domain"</pre>
Remote session identification and authentication succeeds	<pre>May 2 22:45:52 192.0.2.2 Timestamp="2019-05-02 22:45:52", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login succeeded for user admin in domain Shared Domain", SenderType="Management Server", EventId="8376289638658088068", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.login", Result="Success", ObjectName="admin;Shared Domain"</pre>

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Remote session unlocking fails	<pre>May 2 23:03:07 192.0.2.2 Timestamp="2019-05-02 23:03:07", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Wrong password.", SenderType="Management Server", EventId="8376289638658088146", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.password.verificaiton", Result="Fail", ObjectName="admin"</pre>
Remote session unlocking succeeds	<pre>May 2 23:03:36 192.0.2.2 Timestamp="2019-05-02 23:03:36", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Correct password.", SenderType="Management Server", EventId="8376289638658088150", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.password.verificaiton", Result="Success", ObjectName="admin"</pre>
FIA_X509_EXT.1	
Auditable event	Unsuccessful attempt to validate a certificate
Unsuccessful attempt to validate a certificate	<pre>Jun 19 16:08:32 192.0.2.2 Timestamp="2019-06-19 16:08:32", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", InfoMsg="TLS Certificate validation failed. Protocol = TLSv1.2 Peer = [host=198.51.100.6 port=6514] Local = [host=Unknown port=Unknown] - Server certificate is expired", SenderType="Log Server", EventId="7776286620122090328", UserOriginator="System", ClientIpAddress="198.51.100.6", TypeDescription="stonegate.trusted.certificate.validation.failure", Result="Fail"</pre> <pre>Jun 19 16:08:32 192.0.2.2 Timestamp="2019-06-19 16:08:32", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=198.51.100.6 port=6514] Local = [host=192.0.2.2 port=46726] - Syslog authentication failed. [/198.51.100.6:6514] Details: General SSLEngine problem Server certificate is expired", SenderType="Log Server", EventId="7776286620122090329", UserOriginator="System", ClientIpAddress="198.51.100.6", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>
FIA_X509_EXT.1/ITT	
Auditable event	Unsuccessful attempt to validate a certificate

FIA_X509_EXT.1/ITT	
Unsuccessful attempt to validate a certificate (NGFW)	<pre>Jun 18 20:29:55 192.0.2.2 Timestamp="2019-06-18 20:29:55", LogId="10272859", NodeId="192.0.2.4", Facility="Management", Type="Error", CompId="NGFW-FIPS node 1", InfoMsg="self signed certificate in certificate chain (CN = SG Root CA (5a9025c25ef90800))", ReceptionTime="2019-06-18 20:29:55", SenderType="Firewall", SituationId="9000", Situation="FW Communication-Server-Certificate-Error", EventId="6546846308892459099"</pre> <pre>Jun 18 20:29:55 192.0.2.2 Timestamp="2019-06-18 20:29:55", LogId="10272860", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="TLS: Couldn't accept TLS connection (3 192.0.2.2)", ReceptionTime="2019-06-18 20:29:55", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6546846308892459100"</pre>
Unsuccessful attempt to validate a certificate (SMC)	<pre>Jun 19 14:59:32 192.0.2.2 Timestamp="2019-06-19 14:59:32", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.4 port=40158] Local = [port=3020] - Engine authentication failed. [192.0.2.4:40158] Details: General SSLEngine problem No trusted certificate found", SenderType="Log Server", EventId="7776286620122090105", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>
FMT_MOF.1/ManualUpdate	
Auditable event	Any attempt to initiate a manual update
Any attempt to initiate a manual update	<pre>Jul 24 20:52:48 192.0.2.2 Timestamp="2019-07-24 20:52:48", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="You do not have the required permissions to perform this action. Details: You do not have the required permissions to manage Administrators. You are missing the following permissions: - Manage Administrators Change your permissions or contact an administrator with the appropriate permissions to resolve this issue.", SenderType="Management Server", EventId="7766082894518294528", UserOriginator="regularAdmin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.enabled", Result="Fail", ObjectName="admin2"</pre>

FMT_MOF.1/Functions	
Auditable event	Modification of the behavior of the audit functionality when Local Audit Storage Space is full
Modification of the behavior of the audit functionality when Local Audit Storage Space is full	<pre>May 20 14:59:35 192.0.2.2 Timestamp="2019-05-20 14:59:35", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="log_spooling_policy has been modified (discard -> stop).", SenderType="Management Server", EventId="6177649824901365856", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="NGFW-FIPS"</pre>
Modification of the behavior of the transmission of audit data to an external IT entity	<pre>Aug 2 15:44:34 192.0.2.2 Timestamp="2019-08-02 15:44:34", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A new log forward rule was created with All Log Data types to host Audit server (port 6514).", SenderType="Management Server", EventId="5853225097921299210", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.log.forward.new", Result="Success", ObjectName="LogServer 192.0.2.2"</pre>
Modification of the behavior of the handling of audit data	<pre>Aug 2 17:15:00 192.0.2.2 Timestamp="2019-08-02 17:15:00", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="storable_task_definition element has been created.", SenderType="Management Server", EventId="5853225097921299215", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="Delete old log and audit data"</pre> <pre>Aug 2 17:15:33 192.0.2.2 Timestamp="2019-08-02 17:15:33", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="task_schedule element has been created.", SenderType="Management Server", EventId="5853225097921299216", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="(Schedule) Delete old log and audit data"</pre>
FPT_ITT.1	
Auditable event	TLS communication between the distributed TOE components

FPT_ITT.1	
Initiation of the trusted channel (NGFW)	<pre>Jun 18 18:49:40 192.0.2.2 Timestamp="2019-06-18 18:49:40", LogId="10272767", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="TLS: Accepted connection (3 192.0.2.2)", ReceptionTime="2019-06-18 18:49:40", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6546821080254562303"</pre>
Termination of the trusted channel (NGFW)	<pre>Jun 18 18:46:39 192.0.2.2 Timestamp="2019-06-18 18:46:39", LogId="10272744", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="TLS: Connection closed (11 192.0.2.2)", ReceptionTime="2019-06-18 18:48:39", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6546820324340318184"</pre>
Failure of the trusted channel functions (NGFW)	<pre>Jun 18 18:46:49 192.0.2.2 Timestamp="2019-06-18 18:46:49", LogId="10272745", NodeId="192.0.2.4", Facility="Management", Type="Error", CompId="NGFW-FIPS node 1", InfoMsg="ssl3 alert handshake failure", ReceptionTime="2019-06-18 18:48:39", SenderType="Firewall", SituationId="9005", Situation="FW Communication-Communication-Error", EventId="6546820362995023849"</pre> <pre>Jun 18 18:46:49 192.0.2.2 Timestamp="2019-06-18 18:46:49", LogId="10272746", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="TLS: Couldn't establish TLS connection (11 192.0.2.2)", ReceptionTime="2019-06-18 18:48:39", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6546820362995023850"</pre>
Initiation of the trusted channel (SMC)	<pre>Jun 19 14:47:56 192.0.2.2 Timestamp="2019-06-19 14:47:56", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=4987] Local = [host=192.0.2.2 port=51050]", SenderType="Management Server", EventId="7766082894518291231", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.start", Result="Success"</pre>

FPT_ITT.1	
Termination of the trusted channel (SMC)	<pre>Jun 19 14:47:56 192.0.2.2 Timestamp="2019-06-19 14:47:56", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=4987] Local = [port=51050]", SenderType="Management Server", EventId="7766082894518291232", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.end", Result="Success"</pre>
Failure of the trusted channel functions (SMC)	<pre>Jun 19 14:59:32 192.0.2.2 Timestamp="2019-06-19 14:59:32", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.4 port=40158] Local = [port=3020] - Engine authentication failed. [192.0.2.4:40158] Details: General SSLEngine problem No trusted certificate found", SenderType="Log Server", EventId="7776286620122090105", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>
FPT_TUD_EXT.1	
Auditable event	Initiation of update
SMC Appliance update	<pre>May 15 18:33:06 192.0.2.2 Timestamp="2019-05-15 18:33:06", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 15 18:33:06 smca-fips sudo: sgadmin : TTY=unknown ; PWD=/usr/local/forcepoint/smc ; USER=admin ; GROUP=smca_priv ; COMMAND=/usr/bin/sudo /usr/bin/ambr-load -f /usr/local/forcepoint/smc/6.5.5U001.sap", ReceptionTime="2019-05-15 18:33:06", SenderType="Third Party Device", EventId="49163"</pre> <pre>May 15 18:33:06 192.0.2.2 Timestamp="2019-05-15 18:33:06", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 15 18:33:06 smca-fips sudo: admin : TTY=unknown ; PWD=/usr/local/forcepoint/smc ; USER=root ; COMMAND=/usr/bin/ambr-load -f /usr/local/forcepoint/smc/6.5.5U001.sap", ReceptionTime="2019-05-15 18:33:06", SenderType="Third Party Device", EventId="49167"</pre>

FPT_TUD_EXT.1	
SMC Appliance update (continued)	<pre> May 15 18:38:35 192.0.2.2 Timestamp="2019-05-15 18:38:35", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 15 18:38:35 smca-fips sudo: sgadmin : TTY=unknown ; PWD=/usr/local/forcepoint/smc ; USER=admin ; GROUP=smca_priv ; COMMAND=/usr/bin/sudo /usr/bin/ambr-install --no-prompt 6.5.5U001", ReceptionTime="2019-05-15 18:38:35", SenderType="Third Party Device", EventId="49763" May 15 18:38:35 192.0.2.2 Timestamp="2019-05-15 18:38:35", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 15 18:38:35 smca-fips sudo: admin : TTY=unknown ; PWD=/usr/local/forcepoint/smc ; USER=root ; COMMAND=/usr/bin/ambr-install --no-prompt 6.5.5U001", ReceptionTime="2019-05-15 18:38:35", SenderType="Third Party Device", EventId="49767" </pre>
Failed SMC Appliance update	<pre> Jul 24 16:21:46 192.0.2.2 Timestamp="2019-07-24 16:21:46", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Jul 24 16:21:46 smca-fips AMBR_LOGGER.log : ERROR : pid=15000 : Verification failure#012139668755441480:error:21075075:PKCS7 routines: PKCS7_verify:certificate verify error:pk7_smime.c:336:Verify error:self signed certificate#012Traceback (most recent call last):#012 File 'build/lib/ambr_load/application.py' line 126 in _load_local#012 File 'build/lib/ambr_load/application.py' line 260 in _fetch_metadata#012OSError: Verification failure#012139668755441480:error:21075075:PKCS7 routines:PKCS7_verify: certificate verify error:pk7_smime.c:336:Verify error:self signed certificate", ReceptionTime="2019-07-24 16:21:46", SenderType="Third Party Device", EventId="23811" Jul 24 16:21:46 192.0.2.2 Timestamp="2019-07-24 16:21:46",NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Jul 24 16:21:46 smca-fips AMBR_LOGGER.log : ERROR : pid=15000 : Failed to load: /usr/local/forcepoint/smc/6.5.8T066.sap", ReceptionTime="2019-07-24 16:21:46", SenderType="Third Party Device", EventId="23812" Jul 24 16:21:46 192.0.2.2 Timestamp="2019-07-24 16:21:46", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="ERROR: Unable to load /usr/local/forcepoint/smc/6.5.8T066.sap to /var/ambr/downloaded.ERROR: Verification failure139668755441480:error: 21075075:PKCS7 routines:PKCS7_verify:certificate verify error:pk7_smime.c: 336:Verify error:self signed certificateERROR: Failed to load: /usr/local/forcepoint/smc/6.5.8T066.sap", SenderType="Management Server", EventId="7766082894518294145", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.mgtserver.appliance_patch.import", Result="Fail" </pre>

FPT_TUD_EXT.1	
Initiation of NGFW Engine update	<pre>May 15 20:18:39 192.0.2.2 Timestamp="2019-05-15 20:18:39", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Image sg_engine 6.5.3.21205_x86-64-small.zip", SenderType="Management Server", EventId="4392154597657936469", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.engine.upgrade.start", Result="Success", ObjectName="NGFW-FIPS node 1"</pre>
Result of the NGFW Engine update attempt	<pre>May 15 20:21:18 192.0.2.2 Timestamp="2019-05-15 20:21:18", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Image StoneGate firewall(x86-64-small) version 6.5.3 #21205", SenderType="Management Server", EventId="4392154597657936492", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.engine.upgrade.end", Result="Success", ObjectName="NGFW-FIPS node 1"</pre>
Failed NGFW Engine update	<pre>May 15 20:24:03 192.0.2.2 Timestamp="2019-05-15 20:24:03", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Failed to validate Package. Details: /usr/local/forcepoint/smc/tmp/package/ upgrade8013674476078495210.tmp (No such file or directory)", SenderType="Management Server", EventId="4392154597657936504", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.mgtserver.upgrade.import", Result="Fail", ObjectName="Engine Upgrade sg_engine_6.5.2.21155_x86-64-small.zip"</pre>
FTA_SSL.3	
Auditable event	The termination of a remote session by session locking mechanism
Termination of a remote session by session locking mechanism	<pre>May 3 21:25:07 192.0.2.2 Timestamp="2019-05-03 21:25:07", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Management Client window closed due to idle timeout.", SenderType="Management Server", EventId="9192174042956693507", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.session.terminated", Result="Success", ObjectName="admin"</pre>
FTA_SSL.4	
Auditable event	The termination of an interactive session

FTA_SSL.4	
Termination of local administrative session	<pre>May 3 21:17:44 192.0.2.2 Timestamp="2019-05-03 21:17:44", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="May 3 21:17:44 smca-fips login: pam_unix(login:session): session closed for user admin", ReceptionTime="2019-05-03 21:17:44", SenderType="Third Party Device", EventId="4674"</pre>
Termination of remote administrative session	<pre>May 3 21:15:43 192.0.2.2 Timestamp="2019-05-03 21:15:43", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Logout succeeded for user admin.", SenderType="Management Server", EventId="8376289638658089419", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.logout", Result="Success", ObjectName="admin"</pre>
FTA_SSL_EXT.1	
Auditable event	Local session termination
Local session termination	<pre>Jun 18 21:15:56 192.0.2.2 Timestamp="2019-06-18 21:15:56", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Jun 18 21:15:56 smca-fips audispd: node=smca-fips type=PATH msg=audit(1560892556.940:636): item=1 name='/var/run/console/console.lock' inode=1175063 dev=fd:02 mode=0100600 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:pam_var_console_t:s0 nametype=DELETE", ReceptionTime="2019-06-18 21:15:56", SenderType="Third Party Device", EventId="692"</pre> <pre>Jun 18 21:15:56 192.0.2.2 Timestamp="2019-06-18 21:15:56", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Jun 18 21:15:56 smca-fips login: pam_unix(login:session): session closed for user admin", ReceptionTime="2019-06-18 21:15:56", SenderType="Third Party Device", EventId="694"</pre> <pre>Jun 18 21:15:56 192.0.2.2 Timestamp="2019-06-18 21:15:56", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Jun 18 21:15:56 smca-fips audispd: node=smca-fips type=USER_END msg=audit(1560892556.958:637): user pid=3739 uid=0 auid=500 ses=7 subj=system_u:system_r:local_login_t:s0-s0:c0.c1023 msg='op=PAM:session_close acct='admin' exe='/bin/login' hostname=? addr=? terminal=ttty1 res=success'', ReceptionTime="2019-06-18 21:15:56", SenderType="Third Party Device", EventId="695"</pre>

FTP_ITC.1	
Auditable event	Trusted channel functions
Initiation of the trusted channel	<pre>May 2 20:43:56 192.0.2.2 Timestamp="2019-05-02 20:43:56", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=4987] Local = [host=192.0.2.2 port=54854]", SenderType="Management Server", EventId="8376289638658087587", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.start", Result="Success"</pre>
Termination of the trusted channel	<pre>May 2 20:43:56 192.0.2.2 Timestamp="2019-05-02 20:43:56", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=4987] Local = [port=54854]", SenderType="Management Server", EventId="8376289638658087588", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.end", Result="Success"</pre>
Auditable event	Failure of the trusted channel functions
TLS failure	<pre>May 2 22:14:22 192.0.2.2 Timestamp="2019-05-02 22:14:22", NodeId="192.0.2.2",CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.10 port=6514] Local = [host=192.0.2.2 port=48734] - Syslog authentication failed. [/192.0.2.10:6514] Details: Received fatal alert: handshake_failure", SenderType="Management Server", EventId="8376289638658087892", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>
Connection failure	<pre>May 2 22:23:15 192.0.2.2 Timestamp="2019-05-02 22:23:15", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Connection failed : Peer = [host=192.0.2.10 port=6516] - Connection refused: /192.0.2.10:6516", SenderType="Management Server", EventId="8376289638658087950", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.connection.failure", Result="Fail"</pre>
FTP_TRP.1/Admin	
Auditable event	Trusted path functions

FTP_TRP.1/Admin	
Initiation of the trusted path	<pre> Jun 19 15:12:40 192.0.2.2 Timestamp="2019-06-19 15:12:40", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.11 port=48078] Local = [host=192.0.2.2 port=8913]", SenderType="Management Server", EventId="7766082894518291332", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.trusted.connection.start", Result="Success" </pre>
Termination of the trusted path	<pre> Jun 19 15:12:41 192.0.2.2 Timestamp="2019-06-19 15:12:41", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.11 port=48078] Local = [port=8913]", SenderType="Management Server", EventId="7766082894518291334", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.trusted.connection.end", Result="Success" </pre>
Failure of the trusted path functions	<pre> Jun 19 16:19:46 192.0.2.2 Timestamp="2019-06-19 16:19:46", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.11 port=47700] Local = [port=8905] - Client requested protocol TLSv1 not enabled or not supported", SenderType="Management Server", EventId="7766082894518291572", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.trusted.connection.failure", Result="Fail" </pre>
FTP_TRP.1/Join	
Auditable event	Trusted path functions

FTP_TRP.1/Join	
Initiation of the trusted path	<pre>Aug 2 15:15:05 192.0.2.2 Timestamp="2019-08-02 15:15:05", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=60682] Local = [host=192.0.2.2 port=3021]", SenderType="Management Server", EventId="7766082894518302636", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.start", Result="Success"</pre> <pre>Aug 2 15:15:05 192.0.2.2 Timestamp="2019-08-02 15:15:05", LogId="10275793", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="TLS: Connection established (N/A 192.0.2.2)", ReceptionTime="2019-08-02 15:15:05", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6563074533582752721"</pre>
Termination of the trusted path	<pre>Aug 2 15:15:07 192.0.2.2 Timestamp="2019-08-02 15:15:07", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=60682] Local = [port=3021]", SenderType="Management Server", EventId="7766082894518302637", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.end", Result="Success"</pre>
Failure of the trusted path functions	<pre>Aug 2 15:24:42 192.0.2.2 Timestamp="2019-08-02 15:24:42", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.4 port=60688] Local = [port=3021] - Client requested protocol TLSv1.1 not enabled or not supported", SenderType="Management Server", EventId="7766082894518302730", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>
FCO_CPC_EXT.1	
Auditable event	Enabling and disabling communication between the NGFW Engine and SMC.

FCO_CPC_EXT.1	
Enabling from the NGFW Engine	<pre>May 7 13:39:34 192.0.2.4 Timestamp="2019-05-07 13:39:34", LogId="118", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW node 1", InfoMsg="Connection to Management Server (192.0.2.2) enabled", ReceptionTime="2019-05-07 13:46:13", SenderType="Firewall", EventId="6531477451313250422"</pre> <pre>May 7 13:46:11 192.0.2.4 Timestamp="2019-05-07 13:46:11", LogId="220", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW node 1", InfoMsg="Connection to Log Server (192.0.2.2) enabled", ReceptionTime="2019-05-07 13:46:13", SenderType="Firewall", EventId="6531479122055528668"</pre>
Disabling from the NGFW Engine	<pre>May 7 14:12:04 192.0.2.4 Timestamp="2019-05-07 14:12:04", LogId="316", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW node 1", InfoMsg="Engine factory reset initiated from SMC", ReceptionTime="2019-05-07 14:12:04", SenderType="Firewall", SituationId="500", Situation="FW_Notice", EventId="6531485628930982204"</pre> <pre>May 7 14:12:04 192.0.2.4 Timestamp="2019-05-07 14:12:04", LogId="317", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW node 1", InfoMsg="Connection to Management Server (192.0.2.2) and Log Server disabled", ReceptionTime="2019-05-07 14:12:04", SenderType="Firewall", SituationId="500", Situation="FW_Notice", EventId="6531485628930982205"</pre>

FCO_CPC_EXT.1	
Enabling from the SMC	<pre>May 7 13:37:19 192.0.2.2 Timestamp="2019-05-07 13:37:19", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Initial configuration generated for Firewall engine", SenderType="Management Server", EventId="1272623965428252852", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.engine.initial.generate", Result="Success", ObjectName="NGFW"</pre> <pre>May 7 13:39:34 192.0.2.2 Timestamp="2019-05-07 13:39:34", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Initial contact from Firewall Node", SenderType="Management Server", EventId="1272623965428252863", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.engine.initial.contact", Result="Success", ObjectName="NGFW node 1"</pre>
Disabling from the SMC	<pre>May 7 14:12:04 192.0.2.2 Timestamp="2019-05-07 14:12:04", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="1272623965428253087", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.firewall.Reset Engine to Factory Settings", Result="Success", ObjectName="NGFW node 1"</pre> <pre>May 7 14:13:30 192.0.2.2 Timestamp="2019-05-07 14:13:30", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="1272623965428253100", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.delete", Result="Success", ObjectName="NGFW"</pre> <pre>May 7 14:13:30 192.0.2.2 Timestamp="2019-05-07 14:13:30", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="1272623965428253101", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.license.unbind", Result="Success", ObjectName="NGFW node 1"</pre>

Secure the update process

When applying appliance upgrades and patches, review and follow the guidance in the *Forcepoint Next Generation Firewall Product Guide* to ensure that the update is secure.



Note: If the SMC version changes, you must upgrade the Management Client. The process is the same as when installing.

For more information, see the *SMC Appliance maintenance* chapter and the *Upgrading the engines* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

You can download all the installation files that you need to manually upgrade the SMC Appliance or NGFW Engine from <https://support.forcepoint.com/Downloads>.

SMC Appliance and NGFW Engine updates are verified using ECDSA P-521 with SHA-512 digital signatures and a pre-installed public key.

The commands used to update the SMC Appliance verify the digital signature and reject any update that is not valid.

For NGFW Engine updates, the SMC verifies the NGFW Engine update signature when the update is imported to the SMC. Only valid updates can be imported and installed on the NGFW Engine.

Follow these steps to patch the SMC Appliance.



Note: If you are upgrading from an SMC Appliance that has software version 6.4.0 or later, you can use the Management Client to manually import patches that you have downloaded. For more information see the topic *Patch or upgrade the SMC Appliance in the Management Client* in the *SMC Appliance maintenance* chapter in the *Forcepoint Next Generation Firewall Installation Guide*.

Steps

- 1) Download the SMC Appliance patch file (6.5.4P001.sap, for example) from <https://support.forcepoint.com/Downloads>.
- 2) Save the patch file to a USB drive.
- 3) Attach the USB drive to the SMC Appliance, then mount it using the following commands:

```
$ sudo mount /dev/sdb1 /mnt
```

- 4) Load the patch file using the following command:

```
$ sudo ambr-load -f /mnt/6.5.4P001.sap
```

- 5) Install the patch using the following command:

```
$ sudo ambr-install 6.5.4P001
```

- 6) Follow the instructions shown on the screen.

Network processes

Many network processes can run on the appliances while in an evaluated configuration.

For more information, see the *Default communication ports* appendix in the *Forcepoint Next Generation Firewall Product Guide*.

Processes for SMC Appliance

Process	Listening	Ports/Protocol	Contacting	Hardware Privilege	User	Linux Capabilities	TLS	Description
/usr/local/forcepoint/smc/jre/bin/java	DNS Server	53/UDP, 53/TCP	Management Server, Log Server	Ring 3	sgadmin	0	No	DNS queries.
/usr/local/forcepoint/smc/jre/bin/java	Log Server	5514/TCP, 5514/UDP	Monitored third-party components, SMC Appliance	Ring 3	sgadmin	0	No	Syslog reception from third-party components and SMC Appliance.
/usr/local/forcepoint/smc/jre/bin/java	Log Server	3020/TCP	NGFW Engines	Ring 3	sgadmin	0	Server	Log and alert messages; monitoring of blacklists, connections, status, and statistics from NGFW Engines.
/usr/local/forcepoint/smc/jre/bin/java	Log Server	8914-8918/TCP	Management Client	Ring 3	sgadmin	0	Server	Log browsing.
/usr/local/forcepoint/smc/jre/bin/java	Management Server	3021/TCP	Log Server, NGFW Engines	Ring 3	sgadmin	0	Server	System communications certificate request/renewal.
/usr/local/forcepoint/smc/jre/bin/java	Management Server	8902-8903, 8905, 8907, 8913/TCP	Management Client, Log Server	Ring 3	sgadmin	0	Server	Monitoring and control connections.
/usr/local/forcepoint/smc/jre/bin/java	Management Server	8906/TCP	NGFW Engines	Ring 3	sgadmin	0	Server	Monitoring and control connections.
/usr/local/forcepoint/smc/jre/bin/java	Management Server	3023/TCP	Log Server, NGFW Engines	Ring 3	sgadmin	0	Server	Status monitoring.

Process	Listening	Ports/Protocol	Contacting	Hardware Privilege	User	Linux Capabilities	TLS	Description
/usr/local/forcepoint/smc/jre/bin/java	Management Server	8080/TCP	Web browser	Ring 3	sgadmin	0	No	Web Start Management Client
/usr/sbin/snmpd	SMC Appliance	161/UDP	Third-party components	Ring 3	snmp	0xffffffffffff=all	No	Requesting health and other information about the SMC Appliance.
/usr/local/forcepoint/smc/jre/bin/java	Syslog server	6514/TCP	Management Server, Log Server	Ring 3	sgadmin	0	Client	Audit and log data forwarding to syslog servers.
/usr/sbin/snmpd	Third-party components	162/UDP	SMC Appliance	Ring 3	snmp	0xffffffffffff=all	No	Sending SNMP status probing to external devices.
/usr/local/forcepoint/smc/jre/bin/java	Update servers	443/TCP	Management Server	Ring 3	sgadmin	0	Client	Update packages, NGFW Engine upgrades, and licenses.
/usr/bin/python	Update servers	443/TCP	SMC Appliance	Ring 3	root	0xffffffffffff=all	Client	Receiving appliance patches and updates.

Processes for NGFW Engines

Process	Listening	Ports/Protocol	Contacting	Hardware Privilege	User	Linux Capabilities	TLS	Description
/usr/sbin/slapd	Firewall	636/TCP	Management Server	Ring 3	root	0x0000003fffffff	Server	Internal user database replication.
/usr/sbin/authd	Firewall	2543/TCP	Any	Ring 3	root	0x0000003fffffff	No	User authentication (Telnet) for Access rules. Denied by default.
/usr/sbin/upgrd	Firewall	4950/TCP	Management Server	Ring 3	root	0x0000003fffffff	Server	Remote upgrade.
/usr/sbin/mgmttd	Firewall	4987/TCP	Management Server	Ring 3	root	0x0000003fffffff	Server	Management Server commands and policy upload.
/usr/sbin/blacklistd	Firewall	15000/TCP	Management Server	Ring 3	root	0x0000003fffffff	Server	Blacklist entries.

Process	Listening	Ports/Protocol	Contacting	Hardware Privilege	User	Linux Capabilities	TLS	Description
/usr/sbin/smonitd	Firewall	161/UDP	SNMP server	Ring 3	root	0x0000003fffffffff	No	SNMP monitoring.
/usr/sbin/sendlogd	Log Server	3020/TCP	Firewall	Ring 3	root	0x0000003fffffffff	Client	Log and alert messages; monitoring of blacklists, connections, status, and statistics.
/usr/lib/stonegate/bin/contact	Management Server	3021/TCP	Firewall	Ring 3	root	0x0000003fffffffff	Client	System communications certificate request/renewal (initial contact).
/usr/sbin/sendlogd	Management Server	3023/TCP	Firewall	Ring 3	root	0x0000003fffffffff	Client	Monitoring (status) connection.
/usr/sbin/smonitd	SNMP server	162/UDP	Firewall	Ring 3	root	0x0000003fffffffff	No	SNMP traps from the NGFW Engine.
/usr/sbin/dnsmasq	Firewall	53/TCP, 53/UDP	Any	Ring 3	nobody	0x0000003fffffffff	No	DNS relay

