FORCEPOINT

Next Generation Firewall

Common Criteria Evaluated Configuration Guide

6.3.1

Revision E

Contents

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 6.3.1.

The target of evaluation consists of:

- Forcepoint NGFW Security Management Center (SMC) Appliance running software version 6.3.1 with:
  - OpenSSL FIPS Object Module SE #2398 version 2.0.13
  - Bouncy Castle Java API #2768 JCA/JCE provider
- Forcepoint NGFW Engine running software version 6.3.1 with:
  - OpenSSL FIPS Object Module SE #2398 version 2.0.14
  - 1U appliance models: 1101, 1105, 1402, 2101, 2105
  - 2U appliance modes: 3301, 3305
  - 4U appliance model: 6205

Note: Cryptographic modules other than OpenSSL FIPS Object Module SE #2398 version 2.0.13, Bouncy Castle Java API #2768 JCA/JCE provider, 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 6.3, revision A
- *Forcepoint Next Generation Firewall Installation Guide*, version 6.3, revision A
- *How to install Forcepoint NGFW in FIPS mode*, version 6.3, revision C

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 **6.3**.

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	The Management Client is the user interface for the SMC. The Management Client version must match the version of the SMC. **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. 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. • 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	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. 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.
Forcepoint NGFW Engines	NGFW Engine 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.

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*.

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)	• Type • Code
RFC 4443 (ICMPv6)	• Type • Code
RFC 791 (IPv4)	• Source address • Destination address • Transport layer protocol
RFC 2460 (IPv6)	• Source address • Destination address • Transport layer protocol
RFC 793 (TCP)	• Source port • Destination port
RFC 768 (UDP)	• 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.

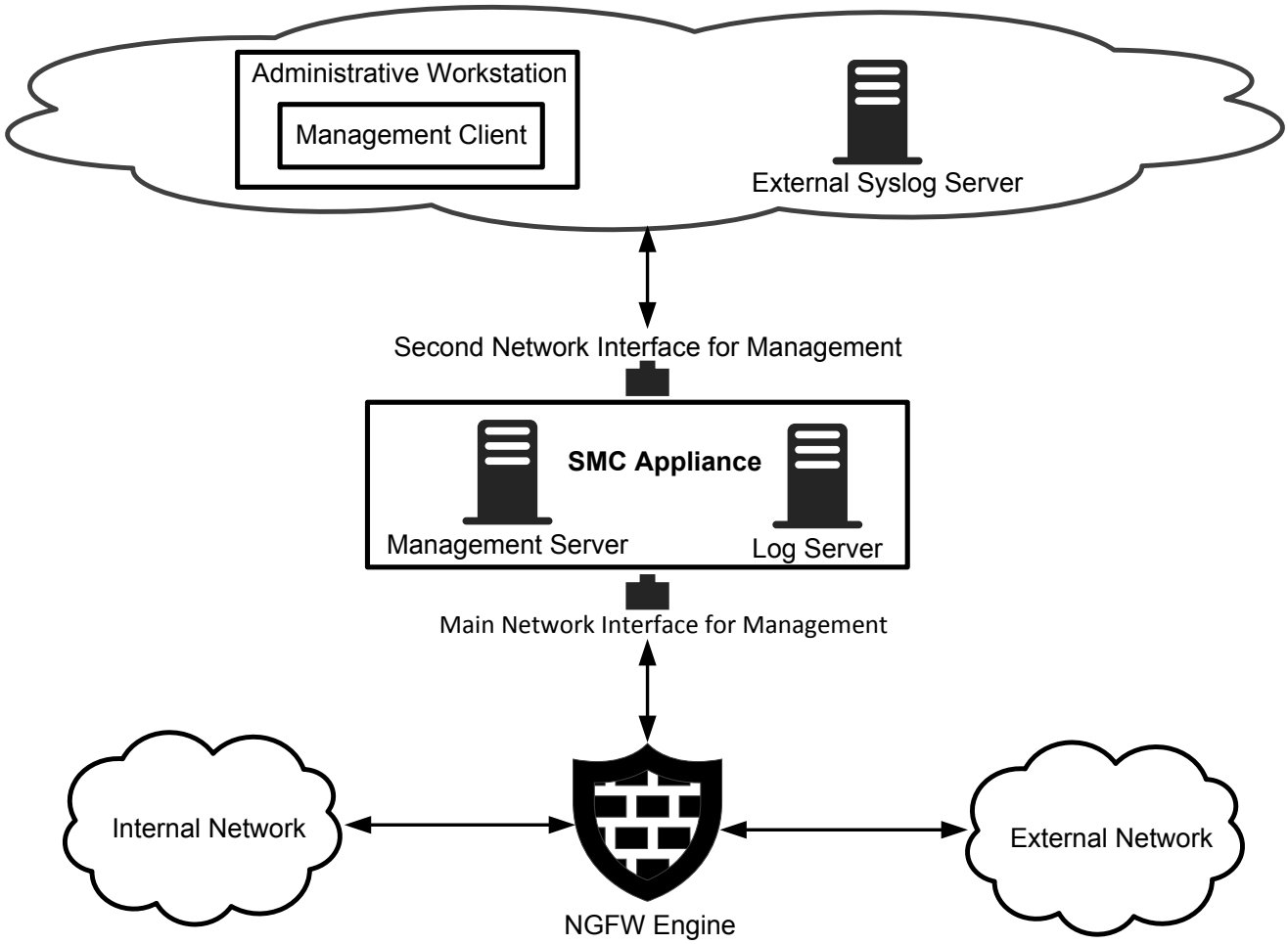
For more information on the FTP Protocol Agent, see the *Define FTP Protocol parameters* topic in the *Working with Service elements* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

For more information on dynamic session establishment capabilities, see the *How Multi-Layer inspection works* 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.

Figure 1: Components overview



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 use the second network interface for management for the connection to the Management Client and external syslog server.

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

If a self-test fails, see the topic about resetting 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 about installing 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	Follow the guidelines in the *Enable NTP on the SMC Appliance* topic in the *Configuring system communications* chapter in the *Forcepoint Next Generation Firewall Product Guide*. To set the date and time manually on the SMC Appliance, enter: `sudo date -s '<YYYY-MM-DD hh:mm:ss>'` where `<YYYY-MM-DD hh:mm:ss>` is the date and time.
Audit Server Configuration	Follow the guidelines in the *Configuring the Log Server* chapter, the *Enabling TLS protection for traffic to external servers* topic in the *Configuring system communications* chapter, and the *Forward audit data from Management Servers to external hosts* topic in the *Reconfiguring the SMC and engines* chapter in the *Forcepoint Next Generation Firewall Product Guide*. 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.

Setting	Configuration

Audit Server Configuration (continued)	**1)** Configure the trusted root CA certificate for the audit server.
	See the *Create Trusted Certificate Authority elements* topic in the *Configuring system communications* chapter in the *Forcepoint Next Generation Firewall Product Guide*
	
	2) If using an imported certificate, configure the trusted CA certificates for the client certificate.
	
	3) If using an imported certificate, generate the client certificate request.
	• See the *Create a certificate request* topic in the *Configuring system communications* chapter in the *Forcepoint Next Generation Firewall Product Guide*.
	• 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.
	
	Note: After creating a certificate request, you must close and re-open the Management Client in order to export the certificate request.
	
	4) Configure the TLS profile using TLS 1.2.
	• The cipher suites that can be used:
	  • TLS_RSA_WITH_AES_128_CBC_SHA
	  • TLS_RSA_WITH_AES_256_CBC_SHA
	  • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	  • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	  • 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.
	
	5) Configure the server identity. Define the following settings for the TLS Server Identity:
	• **TLS Server Identity — DNS Name**
	• **Identity Value** — the DNS name of the audit server.
	
	For more information, see the *Configuring TLS Server Identity* topic in the *Configuring system communications* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

Setting	Configuration
Audit Server Configuration (continued)	If the log or audit data forwarding connection to the audit server is not working, do the following: • 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: `sudo /etc/init.d/sgMgtServer restart` • Restart the Log Server on the local console. Use the command: `sudo /etc/init.d/sgLogServer restart`
Logon Banner	Follow the guidelines in the *Create logon banners for administrators* topic in the *Using the Management Client* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

Administrative Logins	Follow the guidelines in the *Administrator accounts* chapter in the *Forcepoint Next Generation Firewall Product Guide*.
	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.
	To specify the timeout to terminate an inactive local administrative session, enter:
	`TMOUT=<TIMEOUT>;echo "export TMOUT=$TMOUT" >> ~/.bashrc;logger -s -p local3.info "changed console timeout to $TMOUT"`
	where `<TIMEOUT>` is the timeout in seconds.
	For information about setting timeouts in the Management Client, see the *Enable and define password policy settings* topic in the *Administrator accounts* chapter in the *Forcepoint Next Generation Firewall Product Guide*
	To manually log out of the local console account, enter:
	`logout`
	To log out of the Management Client, select **Menu** > **File** > **Exit**.

Password Guidelines	Follow the guidelines in the *Enable and define password policy settings* topic in the *Administrator accounts* chapter in the *Forcepoint Next Generation Firewall Product Guide*. When setting a password, you should select a password that meets these requirements: • 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 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.

Setting	Configuration
Firewall Policy	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 *Creating and managing policy elements* chapter and the *Access rules* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

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** > **Log Handling** branch, for the **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.

2) Save the initial configuration.

   Note: Handle the configuration files securely. They include the one-time password that allows establishing trust with the Management Server.

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 firewall 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.

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 about installing the NGFW Engine in FIPS mode in the document *How to install Forcepoint NGFW in FIPS mode*.

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 about checking the NGFW Engine self-tests in the document *How to install Forcepoint NGFW in FIPS mode*.

Related tasks

Install the NGFW Engine in FIPS mode on page 16

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.
NodeId	IP address of the engine or server that sent the log entry.

Field	Description
Facility	The firewall subsystem that created the log entry.
CompId	The identifier of the creator of the log entry.
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	`Sep 15 10:01:40 192.168.100.110 Timestamp="2017-09-15 10:01:40", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="312949124120969217", UserOriginator="System", ClientIpAddress="192.168.100.110", TypeDescription="audit.start", Result="Success", ObjectName="Audit function started"`  `Sep 15 10:02:00 192.168.100.110 Timestamp="2017-09-15 10:02:00", NodeId="192.168.100.110", CompId="", SenderType="Log Server", EventId="313032317637492737", UserOriginator="System", ClientIpAddress="192.168.100.110", TypeDescription="audit.start", Result="Success", ObjectName="Audit function started"`

FAU_GEN.1.1 a)	
Shutdown of SMC Appliance	Sep 19 12:29:34 192.168.100.110 Timestamp="2017-09-19 12:29:34", NodeId="192.168.100.110", CompId="LogServer 192.168.100.110", SenderType="Log Server", EventId="1831070628459839541", UserOriginator="System", ClientIpAddress="192.168.100.110", TypeDescription="audit.stop", Result="Success", ObjectName="Audit function shutdown" Sep 19 12:29:41 192.168.100.110 Timestamp="2017-09-19 12:29:41", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="1830988869462393028", UserOriginator="System", ClientIpAddress="192.168.100.110", TypeDescription="audit.stop", Result="Success", ObjectName="Audit function shutdown"
Startup of NGFW Engine	Sep 15 01:03:38 192.168.100.63 Timestamp="2017-09-15 01:03:38", LogId="371966", NodeId="192.168.100.63", Facility="System Utilities", Type="Notification", CompId="NGFW node 1", InfoMsg="Auditing log start", ReceptionTime="2017-09-15 15:43:04", SenderType="Firewall", SituationId="78022", Situation="System_Engine-Log-Auditing-State", EventId="6314216882832780542"
Shutdown of NGFW Engine	Sep 15 01:11:26 192.168.100.63 Timestamp="2017-09-15 01:11:26", LogId="372091", NodeId="192.168.100.63", Facility="Management", Type="Notification", CompId="NGFW node 1", InfoMsg="Auditing log end", ReceptionTime="2017-09-15 15:51:53", SenderType="Firewall", SituationId="78022", Situation="System_Engine-Log-Auditing-State", EventId="6314218845632834939"

FAU_GEN.1.1 c)	
Auditable event	Administrative login and logout
Administrative login	Aug 24 13:56:45 192.168.100.110 Timestamp="2017-08-24 13:56:45", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Login succeeded for user Firewall operator in domain Shared Domain", SenderType="Management Server", EventId="1381172142778876437", UserOriginator="System", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.admin.login", Result="Success", ObjectName="Firewall operator;Shared Domain"

FAU_GEN.1.1 c)	

Administrative logout	<pre>Aug 24 13:58:35 192.168.100.110 Timestamp="2017-08-24 13:58:35",
	NodeId="192.168.100.110",
	CompId="Management Server",
	InfoMsg="Logout succeeded for user Firewall operator.",
	SenderType="Management Server",
	EventId="13811721427788764 61",
	UserOriginator="System",
	ClientIpAddress="192.168.230.1",
	TypeDescription="stonegate.admin.logout",
	Result="Success",
	ObjectName="Firewall operator"</pre>

Auditable event	Security related configuration changes

Firewall filtering rule change	<pre>Aug 25 13:42:54 192.168.100.110 Timestamp="2017-08-25 13:42:54",
	NodeId="192.168.100.110",
	RuleId="109.1",
	CompId="Management Server",
	InfoMsg="IPv4 Access Rule @109.1 has been modified.",
	SenderType="Management Server",
	EventId="13811721427788768 43",
	UserOriginator="admin",
	ClientIpAddress="192.168.230.1",
	TypeDescription="stonegate.object.update",
	Result="Success",
	ObjectName="FTP permit"</pre>

FAU_GEN.1.1 c)	
Firewall security policy change	Aug 25 14:07:18 192.168.100.110 Timestamp="2017-08-25 14:07:18", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="1381172142778876880", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="FTP permit" Aug 25 14:07:21 192.168.100.110 Timestamp="2017-08-25 14:07:21", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="1381172142778876881", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.policy.upload.start", Result="Success", ObjectName="FTP permit;NGFW" Aug 25 14:07:37 192.168.100.110 Timestamp="2017-08-25 14:07:37", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="1381172142778876884", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.firewall.policy.upload", Result="Success", ObjectName="NGFW;FTP permit" Aug 25 14:07:37 192.168.100.110 Timestamp="2017-08-25 14:07:37", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="1381172142778876885", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.policy.upload.end", Result="Success", ObjectName="FTP permit;NGFW"
Audit server configuration changes	Aug 25 14:22:37 192.168.100.110 Timestamp="2017-08-25 14:22:37", NodeId="192.168.100.110", 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="1381172142778876905", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.log.forward.new", Result="Success", ObjectName="LogServer 192.168.100.110" Aug 25 14:22:37 192.168.100.110 Timestamp="2017-08-25 14:22:37", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="1381172142778876907", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="LogServer 192.168.100.110"

FAU_GEN.1.1 c)	

Modification of administrator accounts	<pre>Sep 15 17:21:03 192.168.100.110 Timestamp="2017-09-15 17:21:03",
	NodeId="192.168.100.110",
	CompId="Management Server",
	SenderType="Management Server",
	EventId="321549598562728403",
	UserOriginator="admin",
	ClientIpAddress="192.168.230.1",
	TypeDescription="stonegate.object.insert",
	Result="Success",
	ObjectName="admin2"</pre>
	<pre>Sep 15 17:22:09 192.168.100.110 Timestamp="2017-09-15 17:22:09",
	NodeId="192.168.100.110",
	CompId="Management Server",
	SenderType="Management Server",
	EventId="321549598562728405",
	UserOriginator="admin",
	ClientIpAddress="192.168.230.1",
	TypeDescription="stonegate.admin.disabled",
	Result="Success",
	ObjectName="admin2"</pre>
	<pre>Sep 15 17:22:31 192.168.100.110 Timestamp="2017-09-15 17:22:31",
	NodeId="192.168.100.110",
	CompId="Management Server",
	SenderType="Management Server",
	EventId="321549598562728406",
	UserOriginator="admin",
	ClientIpAddress="192.168.230.1",
	TypeDescription="stonegate.admin.enabled",
	Result="Success",
	ObjectName="admin2"</pre>

Auditable event	Changes to time

NTP time change	<pre>Sep 19 22:56:33 127.0.0.1 Timestamp="2017-09-19 22:56:33",
	NodeId="127.0.0.1",
	Type="Notification",
	CompId="3",
	InfoMsg="Sep 19 22:56:33 smca ntpd[10692]: ntpd: Time change.
	Before: Wed Sep 20 13:49:53 After: Tue Sep 19 22:56:33 Peer: 192.168.230.100",
	ReceptionTime="2017-09-19 22:56:33",
	SenderType="Third Party Device",
	EventId="1899"</pre>

Manual time change	<pre>Sep 20 13:17:36 127.0.0.1 Timestamp="2017-09-20 13:17:36",
	NodeId="127.0.0.1",
	Type="Notification",
	CompId="3",
	InfoMsg="Sep 20 13:17:36 smca sudo: admin : TTY=tty1 ; PWD=/home/admin ;
	USER=root ; COMMAND=/bin/date -s 2017-09-20 13:15:01",
	ReceptionTime="2017-09-20 13:17:36",
	SenderType="Third Party Device",
	EventId="1915"</pre>

FAU_GEN.1.1 c)	
Logon banner change	`Sep 19 16:33:43 192.168.100.110 Timestamp="2017-09-19 16:33:43", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Updated Global System Property logon_banner_text to Unauthorized access prohibited", SenderType="Management Server", EventId="1835979995122513620", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="logon_banner_text"`
Minimum password length	`Sep 19 16:37:12 192.168.100.110 Timestamp="2017-09-19 16:37:12", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Updated Global System Property password_character_number_minimum to 10", SenderType="Management Server", EventId="1835979995122513639", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="password_character_number_minimum"`
Remote session timeout change	`Sep 15 18:35:49 192.168.100.110 Timestamp="2017-09-15 18:35:49", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Updated Global System Property lock_screen_setting to true", SenderType="Management Server", EventId="3215495985627286626", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="lock_screen_setting"`
Local session timeout change	`Feb 2 14:46:00 127.0.0.1 Timestamp="2018-02-02 14:46:00", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Feb 2 14:46:00 smca admin: changed console timeout to 60", ReceptionTime="2018-02-02 14:46:00", SenderType="Third Party Device", EventId="5778"`
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**)	`Aug 16 10:22:56 192.168.100.110 Timestamp="2017-08-16 10:22:56", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="7628127771876655218", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.cryptographic_key.new", Result="Success", ObjectName="Audit export key"`

FAU_GEN.1.1 c)	
Certificate signing request	`Aug 16 10:35:08 192.168.100.110 Timestamp="2017-08-16 10:35:08", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="The certificate key from a TLS Credentials was exported. The fingerprint is 34:78:9D:C0:AA:8E:29:00:ED:84:E2:4E:37:BE:1A:4A:81:A1:32:77.", SenderType="Management Server", EventId="7631379044939857923", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.certificate.export", Result="Success", ObjectName="Audit export key"`
Import signed certificate	`Aug 16 13:05:01 192.168.100.110 Timestamp="2017-08-16 13:05:01", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="7628127771876655374", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.cryptographic_key.changed", Result="Success", ObjectName="Audit export key"`
Deletion (from Trash)	`Aug 16 13:13:16 192.168.100.110 Timestamp="2017-08-16 13:13:16", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="7628127771876655382", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.cryptographic_key.deleted", Result="Success", ObjectName="Audit export key"`
Import of a private key and a certificate	`Aug 16 13:32:11 192.168.100.110 Timestamp="2017-08-16 13:32:11", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="7628127771876655399", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.cryptographic_key.new", Result="Success", ObjectName="Audit key pair"`
Auditable event	Resetting passwords
Password reset	`Aug 24 13:35:58 192.168.100.110 Timestamp="2017-08-24 13:35:58", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="1381172142778876218", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.admin.password.change", Result="Success", ObjectName="Firewall operator"`

FCS_TLSC_EXT.1, FCS_TLSS_EXT.2	
Auditable event	TLS sessions
Failure to establish a TLS client session	`Sep 15 17:38:28 192.168.100.110 Timestamp="2017-09-15 17:38:28", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.168.230.100 port=6514] Local = [host=192.168.230.110 port=42510] - Syslog authentication failed. [192.168.230.100/192.168.230.100:6514]Details:General SSLEngine problemGeneral SSLEngine problemNo trusted certificate foundNo trusted certificate found", SenderType="Management Server", EventId="321549598562728500", UserOriginator="System", ClientIpAddress="192.168.230.100", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"`
Failure to establish a TLS server session	`Sep 15 18:08:18 192.168.100.110 Timestamp="2017-09-15 18:08:18", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.168.230.100 port=52423] Local = [port=8902] - Client requested protocol TLSv1 not enabled or not supported", SenderType="Management Server", EventId="321549598562728539", UserOriginator="System", ClientIpAddress="192.168.230.100", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"`

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	`Feb 6 16:39:16 192.168.200.79 Timestamp="2018-02-06 16:39:16", LogId="14999", NodeId="192.168.200.79", Facility="System Utilities", Type="Notification", Srcif="4", CompId="2105 node 1", ReceptionTime="2018-02-06 16:39:16", SenderType="Firewall", SituationId="78023", Situation="System_Engine-NIC-Dropped-RX-Packets", EventId="6366651295280937623"`

FFW_RUL_EXT.1	
Half-open connection limit	Sep 4 18:44:11 192.168.100.63 Timestamp="2017-09-04 18:44:11", LogId="339312", NodeId="192.168.100.63", Facility="Packet Filtering", Type="Notification", Dst="10.0.100.63", CompId="NGFW node 1", InfoMsg="src addrs: 10.1.0.1-10.1.0.5 at least 5 unique addresses", ReceptionTime="2017-09-04 18:44:11", SenderType="Firewall", SituationId="71590", Situation="DOS_SYN-Flood-In-Progress", EventId="6310497514168806737", SfpSynsExpired="208543"

FFW_RUL_EXT.2	
Auditable event	Application of rules configured with the 'log' operation
Permitted traffic	Sep 19 16:17:52 192.168.100.63 Timestamp="2017-09-19 16:17:52", LogId="374091", NodeId="192.168.100.63", Facility="Packet Filtering", Type="Notification", Event="New connection", Action="Allow", Protocol="6", Src="192.168.230.100", Dst="10.0.100.100", Sport="57005", Dport="21", RuleId="107.0", Srcif="2", CompId="NGFW node 1", ReceptionTime="2017-09-19 16:17:53", SenderType="Firewall", SituationId="70018", Situation="Connection_Allowed", EventId="6315896511397888017", Service="FTP" Sep 19 16:17:57 192.168.100.63 Timestamp="2017-09-19 16:17:57", LogId="374092", NodeId="192.168.100.63", Facility="Packet Filtering", Type="Notification", Event="Related connection", Action="Allow", Protocol="6", Src="10.0.100.100", Dst="192.168.230.100", Sport="20", Dport="49399", RuleId="107.0", Srcif="1;1", CompId="NGFW node 1", ReceptionTime="2017-09-19 16:17:58", SenderType="Firewall", SituationId="1004", Situation="FW_Related-Connection", EventId="6315896532872724498", Service="TCP/49399"

FFW_RUL_EXT.2	
Denied traffic	Sep 19 16:21:37 192.168.100.63 Timestamp="2017-09-19 16:21:37", LogId="374189", NodeId="192.168.100.63", Facility="Packet Filtering", Type="Notification", Event="Connection discarded", Action="Discard", Protocol="6", Src="192.168.230.100", Dst="10.0.100.100", Sport="57006", Dport="21", RuleId="108.1", Srcif="2", CompId="NGFW node 1", ReceptionTime="2017-09-19 16:21:38", SenderType="Firewall", SituationId="70019", Situation="Connection_Discarded", EventId="6315897456290693148", Service="FTP"

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Auditable event	All use of identification and authentication mechanism

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Local session identification and authentication failures	Sep 19 13:33:20 127.0.0.1 Timestamp="2017-09-19 13:33:20", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Sep 19 13:33:20 smca login: pam_unix(login:auth): check pass; user unknown", ReceptionTime="2017-09-19 13:33:20", SenderType="Third Party Device", EventId="4605" Sep 19 13:33:20 127.0.0.1 Timestamp="2017-09-19 13:33:20", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Sep 19 13:33:20 smca login: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost=", ReceptionTime="2017-09-19 13:33:20", SenderType="Third Party Device", EventId="4606" Sep 19 13:33:22 127.0.0.1 Timestamp="2017-09-19 13:33:22", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Sep 19 13:33:22 smca login: FAILED LOGIN 1 FROM (null) FOR admin2 Authentication failure", ReceptionTime="2017-09-19 13:33:22", SenderType="Third Party Device", EventId="4607" Sep 19 13:33:27 127.0.0.1 Timestamp="2017-09-19 13:33:27", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Sep 19 13:33:27 smca login: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost= user=admin", ReceptionTime="2017-09-19 13:33:27", SenderType="Third Party Device", EventId="4608" Sep 19 13:33:29 127.0.0.1 Timestamp="2017-09-19 13:33:29", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Sep 19 13:33:29 smca login: FAILED LOGIN 2 FROM (null) FOR admin Authentication failure", ReceptionTime="2017-09-19 13:33:29", SenderType="Third Party Device", EventId="4609"

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Local session successful identification and authentication	Sep 19 13:33:33 127.0.0.1 Timestamp="2017-09-19 13:33:33", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Sep 19 13:33:33 smca login: pam_unix(login:session): session opened for user admin by LOGIN(uid=0)", ReceptionTime="2017-09-19 13:33:33", SenderType="Third Party Device", EventId="4610" Sep 19 13:33:33 127.0.0.1 Timestamp="2017-09-19 13:33:33", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Sep 19 13:33:33 smca login: LOGIN ON tty1 BY admin", ReceptionTime="2017-09-19 13:33:33", SenderType="Third Party Device", EventId="4611"
Remote session identification and authentication failures	Sep 15 18:18:18 192.168.100.110 Timestamp="2017-09-15 18:18:18", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Login attempt for unknown user admin1", SenderType="Management Server", EventId="3215495985627285558", UserOriginator="System", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.admin.login", Result="Fail", ObjectName="Unknown user" Sep 15 18:18:18 192.168.100.110 Timestamp="2017-09-15 18:18:18", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Login attempt for unknown user admin1. From 192.168.230.1.", SenderType="Management Server", SituationId="519", Situation="Management Server: Login failed", AlertSeverity="Low", EventId="1505488698911" Sep 15 18:22:46 192.168.100.110 Timestamp="2017-09-15 18:22:46", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="login failed for user admin. From 192.168.230.1.", SenderType="Management Server", SituationId="519", Situation="Management Server: Login failed", AlertSeverity="Low", EventId="1505488966440" Sep 15 18:22:46 192.168.100.110 Timestamp="2017-09-15 18:22:46", NodeId="192.168.100.110", 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="3215495985627285566", UserOriginator="System", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.admin.login", Result="Fail", ObjectName="admin;Shared Domain"

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Remote session identification and authentication succeeds	Sep 15 18:24:22 192.168.100.110 Timestamp="2017-09-15 18:24:22", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Login succeeded for user admin in domain Shared Domain", SenderType="Management Server", EventId="3215495985627285 72", UserOriginator="System", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.admin.login", Result="Success", ObjectName="admin;Shared Domain"
Remote session unlocking fails	Sep 19 13:56:46 192.168.100.110 Timestamp="2017-09-19 13:56:46", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Wrong password.", SenderType="Management Server", EventId="1835979995122499737", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.password.verification", Result="Fail", ObjectName="admin"
Remote session unlocking succeeds	Sep 19 13:56:48 192.168.100.110 Timestamp="2017-09-19 13:56:48", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Correct password.", SenderType="Management Server", EventId="1835979995122499738", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.password.verification", Result="Success", ObjectName="admin"

FIA_X509_EXT.1	
Auditable event	Unsuccessful attempt to validate a certificate
Unsuccessful attempt to validate a certificate	Sep 15 17:38:28 192.168.100.110 Timestamp="2017-09-15 17:38:28", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="TLS Certificate validation failed.Protocol = TLSv1.2 Peer = [host=192.168.230.100 port=6514] Local = [host=Unknown port=Unknown] - No trusted certificate found", SenderType="Management Server", EventId="3215495985627284 99", UserOriginator="System", ClientIpAddress="192.168.230.100", TypeDescription="stonegate.trusted.certificate.validation.failure", Result="Fail"

FMT_MOF.1(1)	
Auditable event	Modification of the behavior of the audit functionality when Local Audit Storage Space is full

FMT_MOF.1(1)	
Modification of the behavior of the audit functionality when Local Audit Storage Space is full	Sep 19 16:24:33 192.168.100.110 Timestamp="2017-09-19 16:24:33", NodeId="192.168.100.110", CompId="Management Server", SenderType="Management Server", EventId="1835979995122513584", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="NGFW"
Management Server audit storage space becomes full	Feb 7 13:11:53 10.10.10.245 Timestamp="2018-02-07 13:11:53", NodeId="10.10.10.245", CompId="Management Server", InfoMsg="Some files must be deleted in order to free disk space for storage files.", SenderType="Management Server", SituationId="513", Situation="Log Server: disk is becoming full", AlertSeverity="Critical", EventId="1518001913083"
Log Server audit storage space becomes full	Feb 7 10:32:50 10.10.10.245 Timestamp="2018-02-07 10:32:50", NodeId="10.10.10.245", CompId="LogServer 10.10.10.245", InfoMsg="Some files must be deleted in order to free disk space for storage files.", SenderType="Log Server", SituationId="513", Situation="Log Server: disk is becoming full", AlertSeverity="Critical", EventId="1517992370220"
Engine audit storage space becomes full	Feb 7 12:16:39 192.168.200.79 Timestamp="2018-02-07 12:16:39", LogId="6", NodeId="192.168.200.79", Facility="Logging System", Type="System alert", CompId="2105 node 1", InfoMsg="log device 0", ReceptionTime="2018-02-07 12:16:40", SenderType="Firewall", SituationId="10", Situation="System_Log-Spool-Filling", AlertSeverity="Critical", EventId="6366947596753174553"

FPT_TUD_EXT.1	
Auditable event	Initiation of update

FPT_TUD_EXT.1	
SMC Appliance update	Sep 20 09:55:38 127.0.0.1 Timestamp="2017-09-20 09:55:38", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Sep 20 09:55:38 smca sudo: admin : TTY=tty1 ; PWD=/home/admin ; USER=root ; COMMAND=/usr/bin/ambr-load -f /home/admin/6.3.0R001.sap", ReceptionTime="2017-09-20 09:55:38", SenderType="Third Party Device", EventId="1888" Sep 20 10:10:13 127.0.0.1 Timestamp="2017-09-20 10:10:13", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Sep 20 10:10:13 smca sudo: admin : TTY=tty1 ; PWD=/home/admin ; USER=root ; COMMAND=/usr/bin/ambr-install 6.3.0R001", ReceptionTime="2017-09-20 10:10:13", SenderType="Third Party Device", EventId="1900"
Failed SMC Appliance update	Feb 2 14:33:25 127.0.0.1 Timestamp="2018-02-02 14:33:25", NodeId="127.0.0.1",Type="Notification", CompId="3", InfoMsg="Feb 2 14:33:25 smca sudo: admin : TTY=tty1 ; PWD=/home/admin ; USER=root ; COMMAND=/usr/bin/ambr-load -f 6.3.3U001-corrupted.sap", ReceptionTime="2018-02-02 14:33:25", SenderType="Third Party Device", Event Id="5761" Feb 2 14:34:00 127.0.0.1 Timestamp="2018-02-02 14:34:00", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Feb 2 14:33:58 smca AMBR_LOGGER.log : ERROR : pid=10362 : Verification failure#012139875037603656:error:21071065:PKCS7 routines:PKCS7_signatureVerify:digestfailure:pk7_doit.c:1108: #012139875037603656:error:21075069:PKCS7 routines:PKCS7_verify:signaturefailure:pk7_smime.c:400:#012Traceback (most recent call last):#012 File 'build/lib/ambr_load/application.py' line 115 in _load_local#012 File'build/lib/ambr_load/application.py' line 248 in _fetch_metadata#012OSError: Verification failure#012139875037603656:error: 21071065:PKCS7 routines:PKCS7_signatureVerify:digestfailure:pk7_doit.c:1108:#01 2139875037603656:error:21075069:PKCS7 routines:PKCS7_verify:signature failure: pk7_smime.c:400:", ReceptionTime="2018-02-02 14:34:00", SenderType="Third Party Device", EventId="5762" Feb 2 14:34:00 127.0.0.1 Timestamp="2018-02-02 14:34:00", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Feb 2 14:33:59 smca AMBR_LOGGER.log : ERROR : pid=10362 : Failed to load: 6.3.3U001-corrupted.sap", ReceptionTime="2018-02-02 14:34:00", SenderType="Third Party Device", EventId="5763"

FPT_TUD_EXT.1	
Initiation of NGFW Engine update	Aug 25 11:31:17 192.168.100.110 Timestamp="2017-08-25 11:31:17", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Image sg_engine_6.3.0.19023_x86-64-small.zip", SenderType="Management Server", EventId="1381172142778876734", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.engine.upgrade.start", Result="Success", ObjectName="NGFW node 1"
Result of the NGFW Engine update attempt	Aug 25 11:33:22 192.168.100.110 Timestamp="2017-08-25 11:33:22", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Image StoneGate firewall(x86-64-small) version 6.3 #19023", SenderType="Management Server", EventId="1381172142778876762", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.engine.upgrade.end", Result="Success", ObjectName="NGFW node 1"
Failed NGFW Engine update	Sep 19 13:57:27 192.168.100.110 Timestamp="2017-09-19 13:57:27", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Signature verification failed for the Update Package or Engine Upgrade: Details: SHA-512 digest error for image", SenderType="Management Server", EventId="1835979995122499744", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.mgtserver.upgrade.import", Result="Fail", ObjectName="Engine Upgrade sg_engine_6.3.0.19026.corrupted.1_x86-64-small.zip"

FTA_SSL.3	
Auditable event	The termination of a remote session by session locking mechanism
Termination of a remote session by session locking mechanism	Sep 15 18:40:08 192.168.100.110 Timestamp="2017-09-15 18:40:08", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Management Client window closed due to idle timeout.", SenderType="Management Server", EventId="4408721824116899 89", UserOriginator="admin", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.session.terminated", Result="Success", ObjectName="admin"

FTA_SSL.4	
Auditable event	The termination of an interactive session

FTA_SSL.4	
Termination of local administrative session	`Sep 19 14:12:48 127.0.0.1 Timestamp="2017-09-19 14:12:48", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Sep 19 14:12:48 smca login: pam_unix(login:session): session closed for user admin", ReceptionTime="2017-09-19 14:12:48", SenderType="Third Party Device", EventId="4633"`
Termination of remote administrative session	`Sep 15 18:48:02 192.168.100.110 Timestamp="2017-09-15 18:48:02", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="Logout succeeded for user admin.", SenderType="Management Server", EventId="321549598562728673", UserOriginator="System", ClientIpAddress="192.168.230.1", TypeDescription="stonegate.admin.logout", Result="Success", ObjectName="admin"`

FTA_SSL_EXT.1	
Auditable event	Any attempts to establish an interactive session
Failed login on local console	`Feb 2 16:52:55 127.0.0.1 Timestamp="2018-02-02 16:52:55", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Feb 2 16:52:55 smca login: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost= user=admin", ReceptionTime="2018-02-02 16:52:55", SenderType="Third Party Device", EventId="5810"`  `Feb 2 16:52:57 127.0.0.1 Timestamp="2018-02-02 16:52:57", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Feb 2 16:52:57 smca login: FAILED LOGIN 1 FROM (null) FOR admin Authentication failure", ReceptionTime="2018-02-02 16:52:57", SenderType="Third Party Device", EventId="5811"`

FTA_SSL_EXT.1	
Successful login on local console	Feb 2 16:55:05 127.0.0.1 Timestamp="2018-02-02 16:55:05", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Feb 2 16:55:05 smca login: pam_unix(login:session): session opened for user admin by LOGIN(uid=0)", ReceptionTime="2018-02-02 16:55:05", SenderType="Third Party Device", EventId="5812" Feb 2 16:55:05 127.0.0.1 Timestamp="2018-02-02 16:55:05", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Feb 2 16:55:05 smca login: LOGIN ON tty1 BY admin", ReceptionTime="2018-02-02 16:55:05", SenderType="Third Party Device", EventId="5813"

FTP_ITC.1	
Auditable event	Trusted channel functions
Initiation of the trusted channel	Sep 19 15:05:18 192.168.100.110 Timestamp="2017-09-19 15:05:18", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.168.230.100 port=6514] Local = [host=192.168.230.110 port=43158]", SenderType="Management Server", EventId="1835979995122513280", UserOriginator="System", ClientIpAddress="192.168.230.100", TypeDescription="stonegate.trusted.connection.start", Result="Success"
Termination of the trusted channel	Sep 19 15:05:34 192.168.100.110 Timestamp="2017-09-19 15:05:34", NodeId="192.168.100.110", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.168.230.100 port=6514] Local = [host=192.168.230.110 port=43158]", SenderType="Management Server", EventId="1835979995122513282", UserOriginator="System", ClientIpAddress="192.168.230.100", TypeDescription="stonegate.trusted.connection.end", Result="Success"
Auditable event	Failure of the trusted channel functions

FTP_ITC.1	

TLS failure	<pre>Sep 19 14:54:52 192.168.100.110 Timestamp="2017-09-19 14:54:52",
	NodeId="192.168.100.110",
	CompId="LogServer 192.168.100.110",
	InfoMsg="TLS Connection failed : Protocol = NONE
	Peer = [host=192.168.230.100 port=6515]
	Local = [host=192.168.230.110 port=42676] - Syslog authentication failed.
	[192.168.230.100/192.168.230.100:6515]
	Details: Received fatal alert: handshake_failure",
	SenderType="Log Server",
	EventId="1836059194319455236",
	UserOriginator="System",
	ClientIpAddress="192.168.230.100",
	TypeDescription="stonegate.trusted.connection.failure",
	Result="Fail"</pre>

Connection failure	<pre>Sep 19 14:29:50 192.168.100.110 Timestamp="2017-09-19 14:29:50",
	NodeId="192.168.100.110",
	CompId="Management Server",
	InfoMsg="Connection failed :
	Peer = [host=192.168.230.100 port=6515] - Connection refused:
	/192.168.230.100:6515 Details: Connection refused",
	SenderType="Management Server",
	EventId="1835979995122499832",
	UserOriginator="System",
	ClientIpAddress="192.168.230.100",
	TypeDescription="stonegate.connection.failure",
	Result="Fail"</pre>

FTP_TRP.1	
Auditable event	Trusted path functions

Initiation of the trusted path	<pre>Sep 19 15:20:20 192.168.100.110 Timestamp="2017-09-19 15:20:20",
	NodeId="192.168.100.110",
	CompId="Management Server",
	InfoMsg="TLS Connection started : Protocol = TLSv1.2
	Peer = [host=192.168.230.1 port=49215]
	Local = [host=192.168.230.110 port=8913]",
	SenderType="Management Server",
	EventId="1835979995122513305",
	UserOriginator="System",
	ClientIpAddress="192.168.230.1",
	TypeDescription="stonegate.trusted.connection.start",
	Result="Success"</pre>
	<pre>Sep 19 15:20:20 192.168.100.110 Timestamp="2017-09-19 15:20:20",
	NodeId="192.168.100.110",
	CompId="Management Server",
	InfoMsg="Login succeeded for user admin in domain Shared Domain",
	SenderType="Management Server",
	EventId="1835979995122513306",
	UserOriginator="System",
	ClientIpAddress="192.168.230.1",
	TypeDescription="stonegate.admin.login",
	Result="Success",
	ObjectName="admin;Shared Domain"</pre>

FTP_TRP.1	

Termination of the trusted path	<pre>Sep 19 15:45:57 192.168.100.110 Timestamp="2017-09-19 15:45:57",
	NodeId="192.168.100.110",
	CompId="Management Server",
	InfoMsg="Logout succeeded for user admin.",
	SenderType="Management Server",
	EventId="1835979995122513429",
	UserOriginator="System",
	ClientIpAddress="192.168.230.1",
	TypeDescription="stonegate.admin.logout",
	Result="Success",
	ObjectName="admin"</pre>
	<pre>Sep 19 15:45:58 192.168.100.110 Timestamp="2017-09-19 15:45:58",
	NodeId="192.168.100.110",
	CompId="Management Server",
	InfoMsg="TLS Connection ended : Protocol = TLSv1.2
	Peer = [host=192.168.230.1 port=49591] Local = [port=8905]",
	SenderType="Management Server",
	EventId="1835979995122513430",
	UserOriginator="System",
	ClientIpAddress="192.168.230.1",
	TypeDescription="stonegate.trusted.connection.end",
	Result="Success"</pre>

Failure of the trusted path functions	<pre>Sep 19 15:54:28 192.168.100.110 Timestamp="2017-09-19 15:54:28",
	NodeId="192.168.100.110",
	CompId="Management Server",
	InfoMsg="TLS Connection failed : Protocol = NONE
	Peer = [host=192.168.230.100 port=38452]
	Local = [port=8913] - Client requested protocol TLSv1
	not enabled or not supported",
	SenderType="Management Server",
	EventId="1835979995122513436",
	UserOriginator="System",
	ClientIpAddress="192.168.230.100",
	TypeDescription="stonegate.trusted.connection.failure",
	Result="Fail"</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 *Managing SMC Appliance patches* chapter and the *Upgrading the engines* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

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.

Steps

1) Download the SMC Appliance patch file (6.3.1P001.sap, for example) from https://update.stonesoft.com/download/appliance/6.3.0/.

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/6.3.1P001.sap
```

5) Install the patch using the following command:

```
$ sudo ambr-install 6.3.1P001
```

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*.

Table 1: 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.

Process	Listening	Ports/ Protocol	Contacting	Hardware Privilege	User	Linux Capabilities	TLS	Description
/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,NGF 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	3023/TCP	Log Server, NGFW Engines	Ring 3	sgadmin	0	Server	Status monitoring.
/usr/local/forcepoint/smc/jre/bin/java	Management Server	8080/TCP	Web browser	Ring 3	sgadmin	0	No	Web Start Management Client
/usr/sbin/ntpd	NTP server	123/TCP or UDP	SMC Appliance	Ring 3	ntp	0x0000000002000400 =cap_net_bind_service, cap_sys_time	No	Receiving NTP information.
/usr/sbin/snmpd	SMC Appliance	161/UDP	Third-party components	Ring 3	root	0xffffffffffffffff=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	root	0xffffffffffffffff=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	0xffffffffffffffff=all	Client	Receiving appliance patches and updates.

Table 2: Processes for NGFW Engines

Process	Listening	Ports/ Protocol	Contact-ing	Hardware Privilege	User	Linux Capabilities	TLS	Description
/usr/sbin/ slapd	Firewall	636/TCP	Manage-ment Server	Ring 3	root	0x0000003fffffffff	Server	Internal user database replication.
/usr/sbin/ authd	Firewall	2543/TCP	Any	Ring 3	root	0x0000003fffffffff	No	User authentication (Telnet) for Access rules. Denied by default.
/usr/sbin/ upgrd	Firewall	4950/TCP	Manage-ment Server	Ring 3	root	0x0000003fffffffff	Server	Remote upgrade.
/usr/sbin/ mgmtd	Firewall	4987/TCP	Manage-ment Server	Ring 3	root	0x0000003fffffffff	Server	Manage-ment Server commands and policy upload.
/usr/sbin/ blacklistd	Firewall	15000/ TCP	Manage-ment Server	Ring 3	root	0x0000003fffffffff	Server	Blacklist entries.
/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	Manage-ment Server	3021/TCP	Firewall	Ring 3	root	0x0000003fffffffff	Client	System comm-unications certificate request/ renewal (initial contact).
/usr/sbin/ sendlogd	Manage-ment 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