Forcepoint

Next Generation Firewall

6.10

Common Criteria Evaluated Configuration Guide

Revision C

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 on the Forcepoint NGFW Security Management Center Appliance (SMC Appliance) virtual appliance on ESXi 7.0 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 or NGFW virtual appliances on ESXi 7.0.

Evaluated products

The identification for the evaluated product is Forcepoint NGFW 6.10.9.

The target of evaluation consists of:

- Forcepoint NGFW Security Management Center Appliance (SMC Appliance) virtual appliance on ESXi 7.0 with:
  - SMC Appliance software version 6.10.9
  - SMC FIPS Library 1.1.1 (based upon OpenSSL 1.1.1 FIPS)
  - SMC FIPS Java API 1.0.2.3 (based upon Bouncy Castle FIPS Java API JCA/JCE provider)
  - SMC FIPS Cryptographic Module for NTP (based upon NSS Cryptographic Module) version 3.79
- Forcepoint NGFW Engine with:
  - NGFW Engine software version 6.10.9
  - Forcepoint NGFW FIPS Library 1.1.1 (based upon OpenSSL 1.1.1 FIPS)
  - Forcepoint NGFW FIPS Cryptographic Module 1.2.1 (based upon SafeZone FIPS Cryptographic Module)
  - Desktop appliance models: N60, N60L, N120, N120L, N120W, N120WL
  - 1U appliance models: 2201, 2205, 2210
  - 2U appliance modes: 3410, 3405, 3401

- Forcepoint NGFW Engine as a virtual machine on an ESXi 7.0 server

Note

Cryptographic modules other than SMC FIPS Library, SMC FIPS Java API, SMC FIPS Cryptographic Module for NTP, and Forcepoint NGFW FIPS Cryptographic Module 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 6.10, revision C
- *Forcepoint Next Generation Firewall Installation Guide*, version 6.10, revision B
- *How to install Forcepoint NGFW in FIPS mode*, version 6.10, revision D

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
- IPSec VPN Gateway and headend functions

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 SMC Web Access 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.
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 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.

The Forcepoint NGFW system does not support revocation for internal target of evaluation communications between distributed Forcepoint NGFW system components. Certificates are validated as part of the authentication process when they are presented to the Forcepoint NGFW system and when they are loaded into the Forcepoint NGFW system. The following fields are verified as appropriate: signature, validity period, extended key usage, issuer's name, basic constraints (for CA certificates).

Benefits of SMC management

The 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 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)	■ 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

Protocol	Attributes used for matching
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.

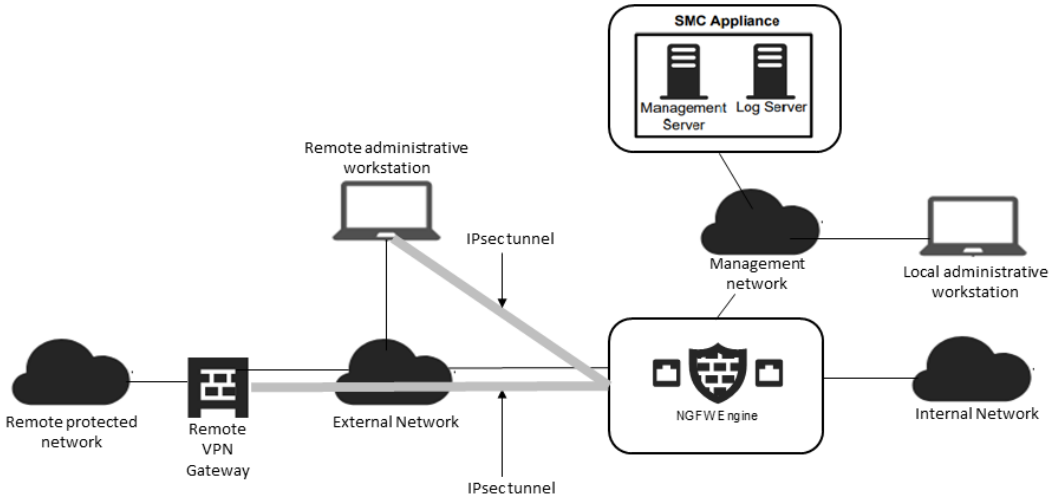
For more information about the FTP Protocol Agent, see the *Define FTP Protocol parameters* topic in the *Working with Service elements* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

For more information about 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.

Components overview



Preparations for the configuration

- Install the NGFW components within a physically protected environment.
- The NGFW is administered over a trusted and separate management network.
- Multiple installations of the NGFW Engine may be used in combination.
- Connect the Virtual SMC Appliance and NGFW Engines to the management network using dedicated management network interfaces.
- Connect the NGFW Engines to the internal and external networks.
- The evaluated configuration includes a virtualization server or virtualization servers where the Virtual SMC Appliance and Virtual NGFW are run in virtual machines.
- Configure the virtual networking according to the network topology.

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
- Install the SMC Appliance as a virtual appliance in ESXi 7.0. Follow the guidelines in the *Installing SMC Appliance software on a virtualization platform* appendix in the *Forcepoint Next Generation Firewall Installation Guide*.
- Access the appliance using the virtual machine console in the VMware Host Client.

The password is not shown while logging on to the local console. No configuration or preparatory steps are required.

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.

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

Related tasks

Configure settings for an evaluated configuration on page 10

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 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	You can set the time manually on the SMC Appliance or you can use NTP time synchronization. By default, the NGFW Engine receives the time from the SMC Appliance. You can optionally also configure NTP time synchronization for the NGFW Engine To use NTP time synchronization, follow the guidelines in the following topics in the *Configuring system communications* chapter in the *Forcepoint Next Generation Firewall Product Guide*: ■ *Create NTP Server elements* ■ *Enable NTP time synchronization on the SMC Appliance* ■ *Enable NTP time synchronization for NGFW Engines*
Time Management (continued)	The NTP implementation for both the SMC Appliance and the NGFW Engine is an NTP client only. NTP clients support communication with NTPv4 servers. By default, the SMC Appliance and NGFW Engine NTP clients do not update their times based on multicast or broadcast NTP packets. The NTP server must use an SHA-1 authentication key. When defining the properties of the NTP Server element, select **SHA1** from the **Key Type** drop-down list. For redundancy, you can configure multiple NTP servers. Create one NTP Server element for each NTP server. When enabling NTP time synchronization on the SMC Appliance, select all of the NTP Server elements.
Time Management (continued)	To set the date and time manually on the SMC Appliance, enter: `sudo date -s '<Day Mon DD hh:mm:ss [TZ] [YYYY]>'` where `<Day Mon DD hh:mm:ss [TZ] [YYYY]>` is the day of week, month, day of month, time, optional time zone and optional year.

Setting	Configuration
Audit Server Configuration	Follow the guidelines in the following topics and chapters in the *Forcepoint Next Generation Firewall Product Guide*: ■ *Configuring the Log Server* chapter ■ *Using certificates to secure communications to external components* topic in the *Managing certificates for system communications* chapter ■ *Forward audit data from Management Servers to external hosts* topic in the *Reconfiguring the SMC and engines* chapter 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. Forcepoint NGFW supports OCSP and CRL revocations for X509v3 certificate validation during negotiation of TLS protected syslog. When handling a certificate bearing OCSP revocation but where Forcepoint NGFW cannot establish a connection with the OCSP responder, Forcepoint NGFW will not accept the certificate (and thus not establish the connection). When handling certificates bearing CRL information but where Forcepoint NGFW cannot establish a connection to the CRL Distribution Point location, Forcepoint NGFW will not accept the certificate as valid. Forcepoint NGFW constructs the certificate path to a trusted certificate, and then verifies the signature, checks the revocation status, validity period, issuer's name, extended key usage and basic constraints for each certificate starting from the trusted certificate.
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 *Managing certificates for system communications* chapter in the *Forcepoint Next Generation Firewall Product Guide*
Audit Server Configuration (continued)	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 *Managing certificates for 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. ■ The target of evaluation generates certificate requests that include a public key, Common Name, Organization, Organizational Unit, Country and device-specific information in the form of Subject Alternative Name. **Note** After creating a certificate request, you must close and re-open the Management Client in order to export the certificate request.

Setting	Configuration
Audit Server Configuration (continued)	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_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. ■ Select **Check Revocation**. ■ You must not select these settings in the evaluated configuration: ■ **Delay CRL Fetching For** ■ **Ignore OCSP Failures For** ■ **Ignore Revocation Check Failures if There Are Connectivity Problems** To use certificate revocation checks, peer certificates must contain the correct CRL Distribution Points extension that refers to a valid CRL Distribution point. The environment must be configured so that the SMC can access the referenced CRL distribution points. If a TLS connection cannot be established because the connection to the CRL server fails, verify the network path to the CRL server and the status of the server, and fix any issues.
Audit Server Configuration (continued)	5) Configure the server identity. Define the following settings for the TLS Server Identity: ■ **TLS Server Identity** — **DNS Name** or **IP Address**. ■ **Identity Value** — the DNS name or IP address of the audit server. For more information, see the *Configure TLS server identity* topic in the *Managing certificates for 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 daemon-ctl restart sgMgtServer` ■ Restart the Log Server on the local console. Use the command: `sudo daemon-ctl restart sgLogServer`
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.

Setting	Configuration
Administrative Logins (continued)	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. To enable temporarily locking administrator accounts after a certain amount of failed logon attempts: 1) In the Management Client, select ☰ **Menu** > **System Tools** > **Global System Properties**. 2) On the **Password Policy** tab, select **Enforce Password Settings for All the Administrators and Web Portal Users**. 3) In the **Logon options** section, select **Temporarily Lock Account After Failed Logon Attempts**. 4) Enter the maximum number of failed logon attempts, and set how long to lock the account for. 5) Click **OK**. **Note** If the administrator account is locked, it is still possible to log on to the SMC Appliance through the local console. To enable and specify the inactivity timeout for remote administrative sessions: 1) In the **Management Client**, select **Menu** > **System Tools** > **Global System Properties**. 2) On the **Password Policy** tab, select **Enforce Password Settings for All the Administrators and Web Portal Users**. 3) In the **Logon options** section, select **Lock the Management Client Window After the User Session is Idle for** and select **Close the Management Client**. 4) Select the time unit and enter the inactivity timeout in the selected time units. 5) Click **OK**. For information about setting timeouts in the Management Client and locking administrator accounts, see the *Enable and define password policy settings* topic in the *Administrator accounts* chapter in the *Forcepoint Next Generation Firewall Product Guide*

Setting	Configuration
Administrative Logins (continued)	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. The minimum password length is configurable from 1 to 80 characters. When operating in a Common Criteria evaluated configuration, we recommend that you set the minimum password length to 15 characters. Configure the **Minimum Number of Required Characters** setting to enforce these recommendations.
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*.

Setting	Configuration
SMC Web Access	If you use the SMC Web Access feature to use the Management Client in a web browser, do the following: 1) Create a TLS Credentials element to use an ECDSA certificate for HTTPS connections for SMC Web Access. Follow the guidelines in the *Create a certificate request* topic in the *Managing certificates for system communications* chapter in the *Forcepoint Next Generation Firewall Product Guide*. a) In the **Subject Alternative Name** field, enter the DNS name or IP address of the SMC Web Access server. b) From the **Public Key Algorithm** drop-down list, select **ECDSA**. c) Configure the other fields in the certificate request as appropriate for your SMC Appliance installation. d) Export the certificate request, sign the certificate request using the trusted CA in your organization, then import the signed certificate back into the SMC. 2) Create a TLS Cryptography Suite Set element, then select only the following algorithms: ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 Follow the guidelines in the *Create TLS Cryptography Suite Set elements* topic in the *Managing certificates for system communications* chapter in the *Forcepoint Next Generation Firewall Product Guide*. 3) On the **SMC Web Access** tab of the Management Server Properties dialog box, select the TLS Credentials element and the TLS Cryptography Suite Set elements to use for SMC Web Access: ■ Select the TLS Credentials element that you created as the value of the **Server Credentials** option. ■ Select the TLS Cryptography Suite Set element that you created as the value of the **Server TLS Cryptography Suite Set** option. Follow the guidelines in the *Enable SMC Web Access* topic in the *Using the Management Client in a web browser* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

Deleting 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.

Set the storage option on the Management Server

The Management Server stores audit and log data locally, and then sends the data to an external audit server.

Below steps help you to set the storage option on the Management Server for deleting the audit data and old logs.

Steps

1) Select **Home**.
2) Browse to **Others** >**Management Server**.
3) Right-click the **Management Server**, then select **Properties**.
4) In the **Log Storage Full** field on the **General** tab, select **Stop receiving**.
5) Click **OK**.

Set the storage option on the Log Server

The Log Server stores audit and log data locally, and then sends the data to an external audit server.

Below steps help you to set the storage option on the Log Server for deleting the audit data and old logs.

Steps

1) Select **Home**.
2) Browse to **Others** >**Log Server**.
3) Right-click the **Log Server**, then select **Properties**.
4) In the **Log Storage Full** field on the **General** tab, select **Stop receiving**.
5) Click **OK**.

Set the storage option on the NGFW Engine

The NGFW Engine stores audit data and old logs temporarily until the data is sent to the Log Server.

Below steps help you to set the storage option on the NGFW Engine for deleting the audit data and old logs which was tested on the evaluated configuration.

Note

Before attempting the steps below, complete the steps for creating an element for the NGFW Engine as explained in section, *Create an element for the NGFW Engine.*

Steps

1) Set the **Log Spooling Policy** option to **Stop Traffic**.

   When the Log Spooling Policy option is set to **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.

2) 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**.

Create a task to delete old log and audit data on SMC

Below steps allow you to set the storage option from SMC for deleting the audit data and old logs:

For more information, see the *Managing and scheduling Tasks* chapter in the *Forcepoint Next Generation Firewall Product Guide*. For more details about the product and how to configure features, click **Help** or press **F1**.

Steps

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 NGFW Engines* 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**.

Limit half-open TCP connections

Forcepoint NGFW can track and maintain the number of half-open TCP connections, and the administrator can define a limit of the number of such connections (either for the NGFW Engine as a whole or for a specific rule).

When the NGFW Engine detects that the threshold has been exceeded, the NGFW Engine denies additional SYN packets. The NGFW Engine will expire such half-open TCP connections after fifteen seconds by default, and the administrator can change this default by configuring the **TCP syn ack seen** timeout.

If a half-open TCP connection limit is not configured the number of concurrent half-open connections is limited only by the TCP timeouts and the concurrent connection capacity of the NGFW appliance.

To limit the number of half-open TCP connections, define the properties in the Engine Editor:

Steps

1) On the **Advanced Settings** > **DoS Protection** branch, set **Rate-Based DoS Protection Mode** to **On**, then set a value between 125 and 100000 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) **(Optional)** On the **Advanced Settings** > **Idle Timeouts** branch, click **Add...** to select **TCP syn ack seen**, and then click **OK**, then enter the value in seconds on the **Idle Timeouts** tab to change the default.

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 about 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.

VPN Configuration

Organizations that want to interconnect their locations using IPSec VPN Gateway, must complete the steps captured in the following sections. Both site-to-site IPsec VPN and a remote access VPN must be configured.

If VPN is broken after the configuration steps, see the *VPN Recovery Instructions* section.

VPN Gateway Settings

Use the Management Client to create the NGFW Engine element. This is described in detail in section *Create an element for the NGFW Engine*. The steps in this section apply to internal VPN gateway. At a high-level configure following:

Steps

1) Configure endpoints with appropriate setting as explained in section, *Define endpoints for VPN Gateway elements*.

2) Define site elements for VPN gateways manually as explained in section, *Defining site elements for VPN gateways manually*.

3) Disable Automated Certificate Management to use an external CA as explained in section *Disable automated certificate management*.

Define endpoints for VPN Gateway elements

Each endpoint is dedicated for one VPN Gateway element.

Any IP address that is already an endpoint for another VPN Gateway element is not shown on the **Endpoints** list for other Gateways that you create for the same NGFW Engine. Each VPN Gateway element can be used in several policy-based VPNs or route-based VPN tunnels. However, you cannot use the same pair of local and remote endpoints in different VPN configurations for the same NGFW Engine.

Steps

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

1) Right-click the Firewall, then select **Edit Single Firewall**.

2) Browse to **VPN** > **Endpoints**.

3) (Optional) Change the selection of IP addresses that you want to use as endpoints in VPNs.
   - Typically, these are IP addresses that belong to interfaces toward the Internet, which are automatically selected based on the firewall's default routing table.
   - If loopback IP addresses are defined for the NGFW Engine, you can select a loopback IP address as the endpoint IP address. On clustered firewalls, the IP addresses are CVIs.
   - (Optional) If you have more than one Internet connection, select an IP address from each ISP.

4) Double-click the endpoint, then configure the following optional settings according to your environment.
   a) (Optional) In the **Name** field, enter a descriptive name for the endpoint.

   b) (Multi-Link tunnels only) From the **Connection Type** drop-down list, select the Connection Type element that defines how the endpoint is used in a Multi-Link configuration.
   You can override these settings in each individual VPN.

   c) (Optional) From the **Use NAT-T** drop-down list, select an option to activate encapsulation for NAT traversal in site-to-site VPNs.
   You might need NAT traversal to traverse a NAT device at the local or at the remote gateway end. The gateway always allows VPN clients to use NAT-T regardless of these settings. NAT-T always uses the standard UDP port 4500.

   Note

   If a private external IP address is translated to a public IP address by an external NAT device, make sure that Contact Addresses and Locations are defined for the Firewall.

5) In the **Phase-1 ID** settings, select an option from the **ID Type** drop-down list according to your environment.
   The ID identifies the Gateways during the IKE SA negotiations.

6) In the **ID Value** field, enter an ID value according to the selected ID type.
   - Distinguished Name to use Distinguished Name (DN). To include an email address in the DN, use the `emailAddress` attribute.
   - IP Address to use SAN: IP address.
   - DNS Name to use SAN: Fully Qualified Domain Name (FQDN)
   - Email to use SAN: user FQDN.

7) (Optional) If the endpoint must use different Phase-1 ID settings in individual policy-based VPNs, add VPN-specific exceptions.
   a) Click **Exceptions**.

   b) Click **Add**, then select the type of ID from the drop-down list.

c) Select a Policy-Based VPN element, then click **Select**.

d) In the **ID Value** cell, enter the value of the ID.

e) Click **OK**.

8) In the **VPN Type** settings, restrict the types of VPNs that the endpoint can be used in.

a) Select **Selected types only**.

b) Select IPsec VPN only.

9) Click **OK** to save your changes to the endpoint.

10) Save the changes.

- To save the changes, click **Save**.
- To save the changes and refresh the security policy on the engine, click **Save and Refresh**.

Disable automatic VPN Site management

Automatic Site management is active by default in the VPN settings for NGFW Engines.

If you prefer not to update the information automatically for any interface, you can disable automatic site management.

When you disable automatic site management, the automatic Site is removed. There must be another Site configured for the gateway for it to be valid in a policy-based VPN.

Steps

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

1) Right-click a Firewall element, then select **Edit Single Firewall**.

2) Browse to **VPN** > **Sites**.

3) Deselect the **Add and Update Addresses Based on Routing** option.

- When the option is not selected, you must manually define the addresses that you want to be routable through the VPN.
- When the option is selected, the Site content updates automatically according to changes made in the routing configuration for the firewall (for interfaces that are not disabled).

4) Click **Save**.

Define a VPN site for internal private networks

You must define site elements for all NGFW Engines and External VPN Gateways that are used in policy-based VPNs.

The site elements must always contain the actual IP addresses that are used inside the VPN tunnel. If traffic in the tunnel is subject to NAT, you must add the NAT addresses to the site. For NGFW Engines, you must add both the NAT addresses and any untranslated IP addresses that are not automatically added to the site. Sites for External VPN Gateways only require the translated address space that the NGFW Engine actually contacts.

The local and remote site definitions must match the same information about the other gateways involved in the VPN because the gateways verify this information during IKE negotiation. When creating VPNs with external Gateways, make sure that the IP address spaces of both gateways are defined identically in the SMC and on the external device. Otherwise, the VPN establishment can fail in one or both directions. Make sure to update the policies of any firewalls that are involved in the VPN when there are changes in the Site elements at either end.

If you want to use a central gateway as a hub that forwards traffic from one VPN tunnel to another, include all IP addresses that are accessible through the central gateway in the central gateway's Site elements.

Note

You cannot add or change Site elements under the VPN Client Gateway element.

Steps

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

1) Right-click the Firewall, then select **Edit Single Firewall** and browse to **VPN** > **Sites**.

2) Select the elements that represent the protected IP addresses behind the gateway, then click **Add** to include them in this site.
   - Do not include IP addresses outside the Gateway's local networks in the site. There is no need to include the Gateways' own IP addresses in the sites. However, there is usually no need to exclude those addresses if they are in the networks you add to the site.
   - IP address ranges might be interpreted differently from lists of IP addresses and networks depending on the VPN device. The system converts Group or Expression elements into address ranges, networks, or individual IP addresses depending on the IP addresses included. Other VPN devices might treat the same types of values differently.
   - VPN Traffic Selector elements allow you to define the IP addresses, protocols, and ports used by a specific host in a VPN site.

3) Click **Save**.

Next steps

If you edited a previously configured VPN, make sure that the configuration of any external VPN gateway device involved contains the same IP address information. Refresh the policy on all affected gateways to transfer the changes.

Disable automated certificate management

Steps

1) Right-click the Firewall, then select **Edit Single Firewall**.

2) Browse to **VPN** > **Certificates** .

3) Deselect **Automated Certificate Management**.

VPN Certificates

You must generate a key pair for authentication, a certificate signing request, and import a signed gateway certificate and trust the CA certificate. Following steps are only the high-level tasks. For more information, see the *Managing VPN Certificates* chapter in the *Forcepoint Next Generation Firewall Product Guide*.

Steps

1) Configure an external CA certificate as trusted as explained in section, *Define additional VPN certificate authorities*.

2) Create a certificate signing request and import a signed certificate for a VPN gateway element as explained in section, *Create a VPN certificate or certificate request for a VPN Gateway element*.

Define additional VPN certificate authorities

To use certificates that are signed by an external CA, define an additional VPN certificate authorities.

Before you begin

You must have the root certificate (or a valid certificate) from the certificate authority.

Note

Only the Internal RSA CA for Gateways and Internal ECDSA CA for Gateways of your SMC are configured as trusted CAs for gateways in VPNs by default. The Internal RSA CA for Gateways is automatically created when you install the SMC.

You can configure the CA as trusted by importing its root certificate or a valid certificate signed by the CA. The certificates must be X.509 certificates in PEM format (Base64 encoding). It might be possible to convert between formats using, for example, OpenSSL or the certificate tools included in Windows.

The CAs you use can be either private (for self-signed certificates) or public (commercial certificate issuers). When you define a CA as trusted, all certificates signed by that CA are valid until their expiration date (or until the CA certificate expires). Optionally, you can also set up the NGFW to check the certificate revocation status from certificate revocation lists (CRLs) or through the OCSP protocol. The CA can cancel a certificate, for example, because it is compromised.

Forcepoint NGFW supports OCSP and CRL revocations for X.509v3 certificate validation during negotiation of IPsec VPN.

Forcepoint NGFW constructs the certificate path to a trusted certificate, and then verifies the signature, checks the revocation status, validity period, issuer's name, extended key usage and basic constraints for each certificate starting from the trusted certificate.

- Revocation status checks using OCSP and CRLs can be enabled independently for each trusted CA.
- The settings are applied to the whole certificate chain excluding the trust anchor.
- When OCSP is enabled but the certificate is not bearing OCSP responder information, or Forcepoint NGFW cannot establish a connection with the OCSP responder, revocation status cannot be determined using OCSP.
- When CRLs are enabled but the certificate is not bearing CRL information, or Forcepoint NGFW cannot establish a connection to the CRL Distribution Point location, revocation status cannot be determined using a CRL.
- When both OCSP and CRLs are enabled but Forcepoint NGFW cannot determine revocation status using OCSP, revocation status is checked using a CRL.
- When either OCSP or CRLs are enabled and Forcepoint NGFW cannot determine the revocation status, Forcepoint NGFW will not accept the certificate as valid.

By default, all CAs you have defined are trusted by all gateways and in all VPNs. If necessary, you can limit trust to a subset of the defined CAs when you configure the VPN Gateway and VPN Profile elements. The trust relationships can be changed at the gateway level and in the VPN Profiles.

To obtain a certificate from an external certificate authority, first create a certificate request.

Steps

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

1) Select **Configuration**, then browse to **SD-WAN**.

2) Browse to **Other Elements** > **Certificates** > **VPN Certificate Authorities**.

3) Right-click **VPN Certificate Authorities**, then select **New VPN Certificate Authority**.

4) On the **General** tab, configure the settings.

Note

All fields but the **Name** on the **General** tab are grayed out. The grayed out fields are always filled in automatically based on information contained in the certificate you import. You cannot change the information in the grayed out fields. The information is shown when you close and reopen the VPN Certificate Authority element after importing the information.

CAUTION

When certificate checking is defined, all certificates signed by the CA are treated as invalid if the validity check cannot be performed. For example, the validity check might not be performed due to incorrectly entered addresses or connectivity problems.

5) On the **Certificate** tab, import the certificate in one of the following ways:
   - Click **Import**, then import a certificate file.

- Copy and paste the information into the field. Include the “Begin Certificate” header and “End Certificate” footer in the information that you copy and paste.

Tip

You can copy and paste the certificate information for many public certificate authorities from the default Trusted Certificate Authority elements. The default Trusted Certificate Authority elements are in the **Configuration** view under **Administration** > > **Certificates** > **Certificate Authorities** > **Trusted Certificate Authorities**.

6) Select **Check Validity** on **Certificate-Specified CRLs** to validate the revocation status of the certificate using a Certificate Revocation List (CRL).

7) Select **Check Validity** on **Certificate-Specified OCSP Servers** to validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP).

8) Click **OK**.

Next steps

If you see an invalid certificate error, the certificate you imported might be in an unsupported format. Try converting the certificate to an X.509 certificate in PEM format (Base64 encoding) using OpenSSL or the certificate tools included in Windows.

If your Firewall Policy is based on the Firewall Template, both LDAP (port 389) and HTTP (port 80) connections from the Firewall are allowed. If your firewall or server configuration differs from these standard definitions, edit the Firewall Policy to allow the necessary connections from the Firewalls.

Create a certificate request for a VPN Gateway element

You can create a certificate request and sign it using an external certificate authority (CA).

Steps

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

1) Select **Configuration**, then browse to **SD-WAN**.

2) Select **VPN Gateways**.
The gateways are displayed.

3) Right-click the VPN Gateway element and select **Tools** > **Generate Certificate**.

4) In the **Generate Certificate** dialog box, enter the certificate information including Common Name, Organization, Organizational Unit, and Country.
   - The target of evaluation generates certificate requests that include a public key, Common Name, Organization, Organizational Unit, Country and device specific information in the form of Subject Alternative Name.
   - The device-specific information includes every IP address, Fully Qualified Domain Name (FQDN), and user FQDN defined as the Phase-1 ID for a VPN endpoint as described in the Define endpoints for VPN Gateway elements section.
   - The target of evaluation performs the asymmetric key generation and includes the public key in the certificate signing request automatically.

5) Enter the Common Name, Organization, Organizational Unit, Country in the dialog.
   - The device-specific information includes every IP address, Fully Qualified Domain Name (FQDN), and user FQDN defined as the Phase-1 ID for a VPN endpoint as described in the *Define endpoints for VPN Gateway elements* section.
   - The target of evaluation performs the asymmetric key generation and includes the public key in the certificate signing request automatically.

6) Select Sign with External Certificate Authority.

7) Select the **Public Key Algorithm** according to the requirements of your organization can be RSA or ECDSA.

8) Select the **Signature Algorithm** that the certificate authority uses to sign the certificate. For RSA select, RSA / SHA-256, RSA / SHA-384, RSA / SHA-512 Signature Algorithm. For ECDSA select, the signature hash algorithm is selected automatically to be ECDSA / SHA-256, ECDSA / SHA-384, or ECDSA / SHA-512, respectively.

9) Enter the **Key Length** for the generated public-private key pair. For RSA, select the 2048, 3072, or 4096 bit Key Length and for ECDSA, select the 256, 384, or 521 Key Length for P-256, P-384, or P-521, respectively.

10) Click **OK**.

    There might be a slight delay while the certificate request is generated.

    The certificate request is added under the gateway in the gateway list.

11) (With external certificate authorities only) Right-click the certificate request, select **Export Certificate Request**, and save it.
   - To generate certificates for a VPN Gateway element, the CA must support PKCS#10 certificate requests in PEM format (Base64 encoding). The signed certificates must also be in the PEM format. It might be possible to convert between formats using, for example, OpenSSL or the certificate tools included in Windows.
   - The CA must be able to copy all attributes from the certificate request into the certificate. In particularly, the X.509 extension Subject Alternative Name must be copied as it is in the request because the value is used for authentication.

12) When you receive the signed certificate, import it by right-clicking on the certificate request and select **Import Certificate**.

13) In the **Import Certificate** dialog box, click **Browse** to open the signed certificate file, or select **As Text** and enter the certificate data. The certificate chain is validated.

14) Click **OK** to import the certificate.

Setup VPN Profile Element

X.509 certificates are used for peer authentication in the evaluated configuration. The predefined VPN Profiles refer to pre-shared key authentication but the evaluation requires X.509 v3 certificate based authentication.

A VPN Profile element is created to select the signature authentication scheme and to specify the settings for IPsec.

- For more detailed steps, see section *Create VPN Profile elements*.

Create VPN Profile elements

If the default VPN Profile elements do not meet your needs, create a custom VPN Profile element.

The options you select are a balance between performance and security. A higher level of security generally requires more processing power.

If External VPN Gateways are involved, you must make sure that all settings match between the gateways.

Steps

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

1) Select **Configuration**, then browse to **SD-WAN**.

2) Browse to **Other Elements** > **Profiles** > **VPN Profiles**.

3) Right-click **VPN Profiles**, then select **New VPN Profile**.

4) Configure the settings.

5) Click **OK**.

VPN Profile Properties dialog box

Use this dialog box to define the properties of a VPN Profile.

Option	Definition
General tab	
Name	The name of the element.
Comment (Optional)	A comment for your own reference.
Overview section	A preview of the selections made on the other tabs is shown.

Option	Definition
IKE SA tab	
Versions	Select the IKEv2 as version. ■ **IKEv2** — Internet Key Exchange version 2.
Cipher Algorithms	Select encryption methods that are appropriate for the sensitivity of the transferred information and any regulations that you might have to follow. Select either one of AES-128 or AES-256 or both. AES-192 is enabled when both AES-128 and AES-256 are selected. ■ **AES-128** — Advanced Encryption Standard CBC Mode algorithm with a 128-bit key size. ■ **AES-256** — Advanced Encryption Standard CBC Mode algorithm with a 256-bit key size.
Message Digest Algorithms	Used for integrity checking and key derivation. Select SHA-2 and 256 as the Minimum Length to enable SHA-256, SHA-384, and SHA-512 for IKE. ■ **SHA-2** — The SHA-2 set of hash functions including SHA-256, SHA-384, and SHA-512.
Diffie-Hellman Groups	Select one or more groups for key exchange. Select from groups 14-21 according to the security requirements for the VPN. ■ **14 (2048 bits)** — Diffie-Hellman key exchange with a 2048-bit modulus. ■ **15 (3072 bits)** — Diffie-Hellman key exchange with a 3072-bit modulus. ■ **16 (4096 bits)** — Diffie-Hellman key exchange with a 4096-bit modulus. ■ **17 (6144 bits)** — Diffie-Hellman key exchange with a 6144-bit modulus. ■ **18 (8192 bits)** — Diffie-Hellman key exchange with a 8192-bit modulus. ■ **19 (ECP 256 bits)** — Diffie-Hellman key exchange with 256-bit elliptic curve. ■ **20 (ECP 384 bits)** — Diffie-Hellman key exchange with 384-bit elliptic curve. ■ **21 (ECP 521 bits)** — Diffie-Hellman key exchange with 521-bit elliptic curve.
Authentication Method	The method that gateways in the VPN use to authenticate to each other. **Note** Select RSA Signatures or ECDSA Signatures as Authentication Method to use X.509 certificates for peer authentication. ■ **RSA Signatures** — Requires that each Gateway has a valid certificate. ■ **ECDSA Signatures** — Requires that each Gateway has a valid certificate. The authentication method you select here is used for site-to-site VPNs. Mobile VPNs have separate settings on the **IPsec Client** tab.
SA Lifetime in Minutes	The time limit after which IKE SA negotiations are done again in a continuously used VPN. This setting also defines the authentication timeout for the Forcepoint VPN Client. Change this setting only if you have a specific reason to do so. The SA lifetime must match the settings of the external gateway device. This setting affects tunnels that carry traffic continuously. Tunnels that are not used are closed after a short delay regardless of the lifetime set. Re-negotiations improve security, but might require heavy processing. The default lifetime is 1440 minutes.

Option	Definition
Always Keep Tunnels Established	When selected, the NGFW Engine keeps the IPsec VPN tunnels established even when no traffic is sent through the VPN tunnel. When the value for the **SA Lifetime in Minutes** option (for IKE SA) or the value for the **IPsec Tunnel Lifetime** (for IPsec SA) option is exceeded, the tunnel is automatically renegotiated even if there is no traffic in the VPN tunnel.

Option	Definition
IPsec SA tab	
IPsec Type	Select one or more options to define integrity checking and data origin authentication for IP datagrams. **Note** Select ESP as the IPsec Type. ■ **ESP** — (Recommended) Encapsulating Security Payload. The communications are encrypted.
Cipher Algorithms	The VPN encryption method. We recommend that you limit the selection to as few choices as possible, preferably only one.. **Note** Select AES-GCM-128, AES-GCM-256, AES-128, and/or AES-256 as Cipher Algorithms. AES-GCM-192 is enabled when both AES-GCM-128 and AES-GCM-256 are selected. Similarly, AES-192 is enabled when both AES-128 and AES-256 are selected. ■ **AES-128** — Advanced Encryption Standard CBC Mode algorithm with a 128-bit key size. ■ **AES-256** — Advanced Encryption Standard CBC Mode algorithm with a 256-bit key size. ■ **AES-GCM-128** — Advanced Encryption Standard Galois/Counter Mode encryption algorithm with a 128-bit key size. Recommended for high-speed networks. ■ **AES-GCM-256** — Advanced Encryption Standard Galois/Counter Mode encryption algorithm with a 256-bit key size. Recommended for high-speed networks.
Message Digest Algorithms	Used for integrity checking, except when authenticated encryption such as AES-GCM is used. We recommend that you select just one of these options if you have no specific reason to select more. **Note** Select SHA-1 and SHA-2 with 256 as the Minimum Length to enable SHA-1, SHA-256, SHA-384, and SHA-512. ■ **SHA-1** — The SHA-1 hash function. ■ **SHA-2** — The SHA-2 set of hash functions including SHA-256, SHA-384, and SHA-512.

Option	Definition
Compression Algorithm	Options for compressing the data in the VPN to reduce the bandwidth use on congested links. ■ **Deflate** — Compresses the data. This compression requires processing and memory resources, which increases latency. Latency might also increase for non-VPN traffic. Do not select this option if the resource utilization is high. Gateways at both ends of each tunnel involved must support the option. ■ **None** — (Recommended for most environments) Sends the data without compressing it. Provides better performance when bandwidth congestion for VPN traffic is not a constant issue or if there is significant processor load.
IPsec Tunnel Lifetime (Optional)	Limits after which IPsec SA negotiations are done again in a continuously used VPN. Reaching either the time or data amount limits triggers new IPsec SA negotiations, which must happen at regular intervals to guarantee security. This setting affects tunnels that carry traffic continuously. Tunnels that are not used are closed after a short delay regardless of the lifetime set here. IPsec SA negotiations are lighter on the processor than IKE SA negotiations, but still require some processing. Too frequent renegotiations can reduce performance down to unacceptable levels. **Note** There is a separate setting for the **SA Lifetime** on the **IKE SA** tab. The SA Lifetime must be longer than the IPsec Tunnel Lifetime. The default is 480 minutes with no limit on the amount of transferred data. The lowest limit that can be configured for the amount of data is 40000 KB.
Security Association Granularity	Defines the level at which security associations (SA) are created. **Note** Select SA per Net as **Security Association Granularity**. ■ **SA per Net** — Creates an SA for each network from which connections are made through the VPN. This setting reduces the overhead when there are many hosts making connections through the VPN.
Use PFS with Diffie-Hellman Group (Optional)	Select one of the Diffie-Hellman groups. We recommend that you select from groups 14-21 according to the security requirements for the VPN. When you use this option, the gateways calculate new values for key negotiations when renegotiating the SAs instead of deriving the values from previously negotiated keying material. This setting increases security if a key is compromised.
Disable Anti Replay Window (Optional)	The anti-replay window feature provides protection against attacks in which packets are replayed. When enabled, the gateway keeps track of the sequence numbers of the arriving packets, and discards any packet whose number matches the number of a packet that has already arrived. It is usually recommended to leave the anti-replay window enabled. However, if QoS is applied to ESP/AH traffic, some of the ESP packets (for the same SA) might be delayed due to the classification and arrive at the destination so late that the anti-replay window has moved too far. This behavior causes the packets to be dropped. In this case, it might be necessary to disable the anti-replay window.

Option	Definition
Disable Path MTU Discovery (Optional)	Prevents the gateway from sending ICMP "Fragmentation needed" messages to the originator when the packet size (including the headers added for IPsec) exceeds the Ethernet-standard 1500 bytes. If this option is selected, packets might be fragmented for transport across the VPN and reassembled at the receiving gateway. Selecting the option might be necessary if ICMP messages do not reach the other gateway or the other gateway does not react to them correctly.

Option	Definition
IPsec Client tab If a VPN Profile that contains VPN client settings is used in a route-based VPN, the VPN Client settings are ignored.	
Authentication Method	Enables certificate-based authentication. This option is always used for the Gateway certificates for the Gateways involved in mobile VPNs, and if certificate authentication is used, also for the client. Certificate authentication does not need separate activation. However, you must configure the issuing authority separately as trusted and you must create certificates for the VPN clients in a manual process. **Note** Select RSA Signatures or ECDSA Signatures as Authentication Method in IKE Authentication to use X.509 certificates for client and gateway authentication. ■ **RSA Signatures** — Requires that each Gateway has a valid certificate. ■ **ECDSA Signatures** — Requires that each Gateway has a valid certificate.
IPsec Security Association Granularity for Tunnel Mode	Defines the level at which security associations (SA) are created in Tunnel Mode. The Forcepoint VPN Client supports only **SA per Net**. ■ **SA per Net** — Creates a security association (SA) for each network from which connections are made through the VPN. This setting reduces the overhead when there are many hosts making connections through the VPN. ■ **Allow SA to Any Network** — (Valid only for third-party IPsec VPN Clients) Select this option together with **SA per Net** to support both the Forcepoint VPN Client and any third-party VPN clients that only support SAs negotiated per Host. ■ **SA per Host** — Creates an SA for each host that makes connections through the VPN. This setting might provide more even load balancing in clusters than the per net setting, but increases the overhead, because per host usually requires more SAs to be negotiated.

Option	Definition
Certificate Authorities tab	
Trust only selected	The gateway trusts only the certificate authorities that you select in the table. You can also restrict trusted CAs in VPN Gateway and External VPN Gateway elements. If you restrict trusted CAs in both the gateway and the VPN Profile, make sure that any two gateways that form a VPN tunnel trust the same CA after all defined restrictions are applied.

Setup external VPN Gateway element

External VPN Gateway elements represent third-party VPN devices or Forcepoint NGFW devices managed by a different Management Server. To use third-party VPN devices or Forcepoint NGFW devices managed by a different Management Server in VPNs, we need to create an External VPN Gateway element. At a high-level configure the following:

1) An external VPN gateway as explained in section, *Create an External VPN Gateway element*.

2) Endpoints for External VPN Gateways as explained in section, *Define endpoints for External VPN Gateways*.

3) VPN site for remote private network as explained in section,*Define a VPN site for remote private networks.*

Create an External VPN Gateway element

External VPN Gateway elements represent third-party VPN devices or Forcepoint NGFW devices managed by a different Management Server. To use third-party VPN devices or Forcepoint NGFW devices managed by a different Management Server in VPNs, create an External VPN Gateway element.

Steps

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

1) Select **Configuration**, then browse to **SD-WAN**.

2) Right-click **VPN Gateways**, then select **New External VPN Gateway**.

3) Configure the settings.

4) Click **OK**.

Define endpoints for External VPN Gateways

Each endpoint is dedicated for one External VPN Gateway element.

Before you begin

You must have an External VPN Gateway element.

Steps

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

1) Right-click the External VPN Gateway element, then select **Properties**.

2) On the **Endpoints** tab, click **Add**.

3) Configure the following optional settings according to your environment if needed.

   a) (Optional) In the **Name** field, enter a descriptive name for the endpoint.

   b) (Policy-Based VPNs only) From the **Connection Type** drop-down list, select an option to define how the endpoint is used in a Multi-Link configuration.

   You can override these settings in each individual VPN.

   c) (Optional) From the **Use NAT-T** drop-down list, select an option to activate encapsulation for NAT traversal in site-to-site VPNs.

   You might need NAT traversal to traverse a NAT device at the local or at the remote gateway end. The gateway always allows VPN clients to use NAT-T regardless of these settings. NAT-T always uses the standard UDP port 4500.

   Note

   If a private external IP address is translated to a public IP address by an external NAT device, make sure that Contact Addresses and Locations are defined for the Firewall.

   d) If necessary, change the default Contact Address or add Exceptions for the Locations of other gateways involved in the VPN.

   The Contact Address must be defined if the IP address for contacting this gateway is different from the IP address that the gateway actually has on its interface (for example, because of NAT).
   Example: An external gateway is behind a NAT device. The real address is defined as the endpoint address, because the IP address is also used as the Phase 1 ID inside the encrypted traffic. Contact must be made using the translated address, so it is defined as a Contact Address.

4) In the **Phase-1** settings, select an option from the **ID Type** drop-down list to according to your environment.

   The ID identifies the Gateways during the IKE SA negotiations. The **IP Address** might not work as an ID if the address is translated using NAT.

5) In the **ID Value** field, enter an ID value according to the selected ID type.

   - Distinguished Name to use Distinguished Name (DN) .
   - IP Address to use SAN: IP address.
   - DNS Name to use SAN: Fully Qualified Domain Name (FQDN).
   - Email to use SAN: user FQDN.

   Note

   Make sure that the ID value matches the identity configured on the external gateway device.

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

Define a VPN site for remote private networks

You must define site elements for all NGFW engines and external VPN gateways that are used in policy-based VPNs.

The Site elements must always contain the actual IP addresses that are used inside the VPN tunnel. If traffic in the tunnel is subject to NAT, you must add the NAT addresses to the site. For NGFW Engines, you must add

both the NAT addresses and any untranslated IP addresses that are not automatically added to the site. Sites for External VPN Gateways only require the translated address space that the NGFW Engine actually contacts.

The local and remote site definitions must match the same information about the other gateways involved in the VPN because the gateways verify this information during IKE negotiation. When creating VPNs with external Gateways, make sure that the IP address spaces of both gateways are defined identically in the SMC and on the external device. Otherwise, the VPN establishment can fail in one or both directions. Make sure to update the policies of any firewalls that are involved in the VPN when there are changes in the Site elements at either end.

If you want to use a central gateway as a hub that forwards traffic from one VPN tunnel to another, include all IP addresses that are accessible through the central gateway in the central gateway's Site elements.

Note

You cannot add or change Site elements under the VPN Client Gateway element.

Steps

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

1) Select **Configuration**, then browse to **SD-WAN**.

2) Browse to **VPN Gateways**.

3) Right-click External VPN Gateway, then select **New** > **Site**.

4) Select the elements that represent the protected IP addresses behind the Gateway, then click **Add** to include them in this site.
   - Do not include IP addresses outside the Gateway's local networks in the site. There is no need to include the Gateways' own IP addresses in the sites. However, there is usually no need to exclude those addresses if they are in the networks you add to the site.
   - IP address ranges might be interpreted differently from lists of IP addresses and networks depending on the VPN device. The system converts Group or Expression elements into address ranges, networks, or individual IP addresses depending on the IP addresses included. Other VPN devices might treat the same types of values differently.
   - VPN Traffic Selector elements allow you to define the IP addresses, protocols, and ports used by a specific host in a VPN site.

5) Click **OK**.

Settings for VPN clients

You can configure authentication settings and virtual IP address management for remote VPN clients.

Idle timeout:To terminate a VPN client session after a period of inactivity, set the **Authentication Idle Time-Out**.

1) Right-click an NGFW Engine, then select Edit <element type>.

2) Browse to **Add-Ons** > **User Authentication**.

3) Enter the **Authentication Idle Time-Out** in seconds.

Virtual Address: To assign an internal IP address to the VPN client, configure a DHCP server for the firewall.

Activate the internal DHCP server on a firewall interface

You can use the internal DHCP server in firewall to assign IPv4 addresses to hosts in the protected network.

Note

You can use the internal DHCP server to provide IP addresses to the VPN client only if you use Single Firewalls as VPN gateways.

Steps

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

1) Right-click an NGFW Engine, then select **Edit Single Firewall**.
2) Browse to **Interfaces**.
3) Right-click a Physical Interface, then select **Edit Physical Interface**.
4) On the **DHCPv4** tab, select **DHCPv4 Server** from the **DHCP Mode** drop-down list.
5) Configure the settings, then click **OK**.
6) Click **Save and Refresh** to transfer the new configuration to the NGFW Engine.

Define a DHCP Server

A DHCP Server dynamically assigns IP addresses.

Steps

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

1) Select **Configuration**, then browse to **Network Elements**.
2) Browse to **Servers**.
3) Right-click **Servers**, then select **New** > **DHCP Server**.
4) In the **Name** field, enter a unique name.
5) Add the IPv4 address of the interface the internal DHCP server is configured on.
6) Click **OK**.

Define virtual IP addresses for VPN clients

You can use assign the VPN client an IP address in the VPN, independent of the address the VPN client computer uses in its local network.

Before you begin

To use virtual IP addresses for VPN clients:

- You can use the internal DHCP server to provide IP addresses to the VPN client Virtual Adapter only if you use Single Firewalls as VPN gateways.
- The users must use a VPN client that has a Virtual Adapter feature. The Forcepoint VPN Client always has this feature installed and active.

The virtual IP address is only used in communications through the VPN tunnels. The VPN gateway gets the IP address and network settings of the VPN client from the DHCP server and forwards the information to the VPN client.

Steps

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

1) Right-click the firewall, then select **Edit Single Firewall**.

2) Browse to **VPN** > **VPN Client**.

3) From the **DHCP Mode** drop-down list, select Relay.

4) From the **Interface** or **Interface for DHCP Relay** drop-down list, select the source address for the DHCP packets when querying the DHCP server (the interface toward the DHCP server).

5) Click **Add**, then select the DHCP server element that assigns IP addresses for the VPN clients.

6) (Optional) From the **Add Information** drop-down list, select what VPN Client user information is added to the Remote ID option field in the DHCP Request packets.
   - **Add User information** — VPN Client user information (in the form user@domain) is automatically added to the Remote ID option field in the DHCP Request packets.
   - **Add Group information** — VPN Client user information (in the form group@domain) is automatically added to the Remote ID option field in the DHCP Request packets.

   Your DHCP server must support the **DHCP Relay Agent Information** option to use this information. Depending on your DHCP server configuration, this information can be used as a basis for IP address selection.

7) (Optional) Select **Restrict Virtual Address Ranges**, then enter the IP address range in the field on the right.

8) (Optional) Configure the Firewall to act as a proxy for the VPN client's ARP requests.
   a) Select **Proxy ARP**.

b) In the field on the right, enter the IP address range for proxy ARP.

Note

The **Proxy ARP** option might be required for a working VPN depending on your network configuration.

9) Click **Save and Refresh**.

Note

You must restrict the local DHCP service to the VPN client virtual IP address use. For details, refer section *Restrict the local DHCP service*.

Set up users for certificate based authentication

The Management Server includes an integrated LDAP directory for storing user information.

When the Management Server's internal LDAP directory is used, the user and user group information is stored on the Management Server. Each firewall node stores a replica of the user database, and any changes to the main database are replicated immediately to the firewalls. This way, the firewalls can access their local directories instead of constantly communicating user information over the network.

Create User elements

The User element defines who your users are and how they can identify themselves to get access to networks and services as defined in your Firewall Access rules.

You create Users as members of a User Group. You do not have to specify all user parameters separately for each individual User. A User that is a member of a User Group can inherit, for example, the Authentication Method and account expiration time from the User Group. Each User Group must belong to an LDAP Domain. We recommend creating a separate user account used for each user. Each user can belong to several User Groups within the LDAP Domain. User-specific properties can override properties defined at the User Group level.

You can import and export Users and User Groups through an LDIF file to or from some other Management Server.

Note

Although you cannot edit User Group memberships in the User element properties, each user can belong to several User Groups. After creating the User element, drag and drop it to other User Groups to add more group memberships.

Steps

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

1) Select **Configuration**, then browse to **User Authentication**.

2) Browse to **Users**.

3) Add a user to a User Group in one of the following ways:

- Right-click a User Group and select **New** > **Internal User** (for the internal **stonegate** parent group).

- Right-click a User Group and select **New Internal User** (for a User Group under the internal **stonegate** parent group).

4) In the **Name** field, enter a unique name to identify the User in the directory.

   The name is used as the common name (CN) for the User. The distinguished name (DN) is inherited from the LDAP Domain to which the User belongs. The DN and CN in the internal LDAP database can be different from the DN in the user certificate when using certificate based authentication.

5) (Optional) Change the Activation settings for the user account.

6) Click the **Authentication** tab.

7) Click **Add** to select the client certificate in **Authentication Methods** for the user.

8) Enter the user identifier in the **Subject**, Alternative Name, or CN field.

Note

When Distinguished Name is used, it must be entered in a specific format where the components are separated with a comma and exactly one space character, and there are no spaces around the equality signs. For example "DC=com, DC=example, CN=Lisa Smith". The OpenSSL x509 tool shows Distinguished Names in the desired format when using option "-nameopt utf8". For example, run "`openssl x509 -text -nameopt utf8 -noout -in certificate.pem`" and look for the Subject line in the output. When an IPv6 address from the Subject Alternative Name list is used, it must be entered in the short format and in lowercase, as described in Section 4 of RFC 5952. For example the IPv6 Address 2001:DB8:0:125:150:10:1:111 should be entered as 2001:db8::125:150:10:1:111.

9) Click **OK**.

Result

The user account is created. If the user is stored in the internal LDAP database, the information is automatically synchronized to the local databases on the Firewalls unless user database replication has been disabled.

Set user database replication on for Firewalls

The internal user database on the Management Server is replicated automatically to Firewall engines.

The engine uses the local copy of the internal user database to authenticate users without a connection to the Management Server. If you have a reason to do so, you can turn off the replication.

CAUTION

If you want to prevent users from authenticating, remove the authentication settings of a user instead of turning off the replication. Turning off the replication prevents any new users you add after the operation from authenticating, but might not prevent existing users from doing so.

Steps

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

1) Right-click a Single Firewall, Firewall Cluster, or Master NGFW Engine and select or deselect **Options** > **User DB Replication**.

Reset a firewall's local user database

You can replace the firewall's local copy of the user database with a copy of the internal user database on the Management Server.

If you use the internal user database of the SMC, the user information is stored centrally on the Management Server. When changes are made, they are incrementally replicated to each firewall node to guarantee fault-tolerant authentication. If necessary, you can perform a full synchronization manually.

Steps

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

1) Right-click a Single Firewall or individual nodes of a Firewall Cluster and select **Commands** > **Reset User Database**.

2) Click **Yes** in the Confirmation message.

   The node's local copy of the user database is replaced with a copy of the internal user database on the Management Server.

Define policy based VPN elements

The Policy-Based VPN element collects together the gateways and the VPN Profile, and provides the settings for defining the topology and the tunnels of the policy-based VPN.

Both site-to-site and mobile client can be in the same VPN.

Define a site-to-site VPN

The Policy-Based VPN editing view has three tabs. The gateway selection on the **Site-to-Site VPN** tab determines the following:

- Which gateways are included in the VPN.
- Which gateways form tunnels with each other.
- Which gateways contact each other through a hub gateway instead of contacting each other directly.

You define general VPN topology by classifying gateways as Central Gateways or Satellite Gateways. This classification defines which tunnels are generated on the **Tunnels** tab, and which gateways can be selected for mobile VPN access on the **Mobile VPN** tab.

IPv4 Access rules control which connections use the VPN tunnels. Always check the Access rules after you add or remove tunnels.

Note

Each endpoint-to-endpoint tunnel can only exist in one active VPN. If you use the same two gateway elements in more than one VPN, make sure that the topology does not create duplicate tunnels. You can also disable any duplicates of existing tunnels on the **Tunnels** tab.

Steps

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

1) Select **Configuration**, then browse to **SD-WAN**.

2) Browse to **Policy-Based VPNs**.

3) Right-click the Policy-Based VPN element, then select **Edit**.

4) On the **Site-to-Site VPN** tab, drag and drop the Gateways you want to include in this VPN into either of the two panes for the VPN topology.
   - If you add a gateway under **Central Gateways**, the gateway can establish a VPN with any other gateway in the VPN. The **Tunnels** tab is populated with tunnels between the endpoints of the gateway you add and the endpoints of all other gateways in the VPN.
   - If you add a gateway under **Satellite Gateways**, the gateway can establish a VPN only with central gateways in this VPN. The **Tunnels** tab is populated with tunnels between the endpoints of the gateway you add and the endpoints of the central gateways.
   - The **Issues** pane alerts you to any incompatible or missing settings that you must correct.

   Note

   Be careful to not unintentionally drop gateways on top of other gateways. Dropping gateways on top of other gateways creates a forwarding relationship on a hub gateway.

5) (Optional) If you want to forward connections from one VPN tunnel into another through a hub gateway, drag and drop a gateway on top of another gateway. The gateway is added under the other gateway at the same level as the Sites.

   The Gateway used as a hub requires a special Site configuration.

6) (Optional) If you want to exclude a gateway's Site (some IP addresses) from this VPN, right-click the Site element under the gateway, then select **Disable.**

7) (Optional) Define which VPN Gateways provide Mobile VPN access.
   a) On the **Mobile VPN** tab, select one of the following options:
      - **Only central Gateways from overall topology** — Only the VPN Gateways in the **Central Gateways** listed on the **Site-to-Site VPN** tab provide mobile VPN access.
      - **All Gateways from overall topology** — All VPN Gateways included in the VPN provide mobile VPN access.
      - **Selected Gateways below** — Only the VPN Gateways that you add to the **Mobile VPN Gateways** tree provide mobile VPN access. Drag and drop the VPN Gateways from the **Resources** pane.

8) Click **Save**.

Define a mobile VPN for remote clients

In a mobile VPN, a VPN client on a user's device connects to a VPN gateway.

Steps

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

1) Configure VPN Client settings in the Engine Editor as explained in chapter Settings for VPN clients.

2) Click **Save and Refresh** to save the changes to the configuration and refresh the policy on the engine.

3) Create a policy-based VPN or edit an existing policy-based VPN.

4) On the **Mobile VPN** tab of the policy-based VPN, select **Only central Gateways from overall topology** to define which VPN Gateways provide Mobile VPN access:
   - **Only central Gateways from overall topology** — Only the VPN Gateways in the **Central Gateways** list on the **Site-to-Site VPN** tab provide mobile VPN access.

5) Click **Save**.

Setup VPN access rules

The Access rules define which traffic is sent to the policy-based VPN and which traffic is allowed out of the policy-based VPN.

No traffic is sent out through the policy-based VPN until you direct traffic to the VPN in the Access rules.

Add rule for the site-to-site VPN

A site-to-site VPN is created between two or more gateway devices that provide VPN access to several hosts in their internal networks. Site-to-site VPNs are supported for IPv4 and IPv6 traffic.

You must define access rules to control encryption and decryption of traffic between local and remote site.

Add a rule or rules to encrypt traffic from the local site to the remote site

Steps

1) Select **Configuration**.

2) Browse to **NGFW** > **Policies** > **Firewall Policies**.

3) Right-click the Firewall policy that is used by the NGFW Engines involved in the VPN, then select **Edit Firewall Policy**.

4) Add two IPv4 or IPv6 Access rules in a suitable location in the policy.
   - Make sure that rules for sending traffic through the VPN are above other rules that match the same traffic the **Allow**, **Discard**, or **Refuse** action.
   - Traffic that you do not want to send through the VPN must not match these rules. Traffic that is not routable through the VPN is dropped if it matches these rules.

5) Fill in the rules as outlined here. If NAT is enabled in the VPN, remember that the Access rules are checked before the NAT rules are applied.

   Example VPN rules

Source	Destination	Service	Action
Networks or hosts of the local site	Networks or hosts of the remote site	Set as needed.	Select **Allow**, then open the Action options. Set **VPN Action** to **Enforce VPN**, then select a Policy-Based VPN.
Remote internal networks	Local internal networks	Set as needed.	Select **Allow**, then open the Action options. Set **VPN Action** to **Enforce VPN**, then select a Policy-Based VPN.

6) Save the policy.

7) Refresh the policies of all firewalls involved in the VPN to activate the new configuration.

Add a rule or rules to decrypt traffic from the remote site to the local site

Steps

1) Select **Configuration**.

2) Browse to **NGFW** > **Policies** > **Firewall Policies**.

3) Right-click the Firewall policy that is used by the NGFW Engines involved in the VPN, then select **Edit Firewall Policy**.

4) Add two IPv4 Access rules in a suitable location in the policy.
   - Make sure that rules for sending traffic through the VPN are above other rules that match the same traffic the **Allow**, **Discard**, or **Refuse** action.
   - Traffic that you do not want to send through the VPN must not match these rules. Traffic that is not routable through the VPN is dropped if it matches these rules.

5) Fill in the rules as outlined here. If NAT is enabled in the VPN, remember that the Access rules are checked before the NAT rules are applied.

   Example VPN rules

Source	Destination	Service	Action
Networks or hosts of the remote site	Networks or hosts of the local site	Set as needed.	Select **Allow**, then open the Action options. Set **VPN Action** to **Enforce VPN**, then select a Policy-Based VPN.

6) Save the policy.

7) Refresh the policies of all firewalls involved in the VPN to activate the new configuration.

Add rule to decrypt from remote VPN clients

Authentication is always required to establish a VPN tunnel. VPN client connections are matched based on Source, Destination, and Service like any other traffic. The example rule matches only specific users and only after the users have already successfully authenticated. We recommend always adding the authentication requirement to rules that are specific to VPN clients.

After the VPN tunnel is established, any connection from the VPN clients to the internal network is matched against the Access rules as usual.

Setup access rules to decrypt traffic from remote VPN clients

Steps

1) Select **Configuration**.

2) Browse to **NGFW** > **Policies** > **Firewall Policies**.

3) Right-click the Firewall policy that is used by the NGFW Engines involved in the VPN, then select **Edit Firewall Policy**.

4) Add an IPv4 Access rule in a suitable location in the policy and configure the rule as outlined here:

Example VPN rule

Source	Destination	Service	Action	Authentication
Network element that represents the virtual IP address range for the VPN Client	Networks or hosts of the local site	Set as needed.	Select **Allow**, then open the Action options. Set **VPN Action** to **Enforce VPN**, then select a Policy-Based VPN.	Users: The User Group or User elements Authentication Methods: Client Certificate

5) Save the policy.

6) Refresh the policies of all firewalls involved in the VPN to activate the new configuration.

Modify firewall policy template

Modify the firewall policy template to restrict remote VPN client sessions based on location, time, and day.

Following points are to be noted:

- You can specify when access rules are enforced.

- You specify rule validity times using Rule Validity Time elements.
- You can use the same Rule Validity Time element in multiple rules and policies.
- You can also create several Rule Validity Time elements and use the elements in one rule.

Steps

1) Select **Configuration**.
2) Right-click **Rule Validity Time**, then select **New Rule Validity Time**.
3) Configure the settings. Specify using the **Active** option when VPN client sessions are denied. Select either **Between These Times of the Day**, or **On These Days of the Week**.
4) Click **OK**.
5) Open the Firewall cPP Template for editing.
6) Before the `Automatic Rules Insert Point`, add the following rule:

```
Source: Networks or hosts are denied locations
Destination: $$ Local Cluster
Service: ISAKMP (UDP), NAT-T (Destination)
Action: Discard
Time: The Rule Validity Time elements
```

7) Save the policy template.
8) Refresh the policies of all firewalls involved in the VPN to activate the new configuration.

Restrict the local DHCP service

Restrict the local DHCP service to the VPN client virtual IP address use.

Steps

1) Create the following Expression Network element "Node-internal" (negation of the built-in Zone element):

```
~Node-internal
```

2) Open the Firewall cPP Template for editing.
3) Before the **Automatic Rules Insert Point**, add the following rule:

```
Source: NOT Node-internal
Destination: $$ Valid DHCP Servers for Mobile VPN clients, DHCP Broadcast Destination
Service: BOOTPS (UDP)
Action: Discard
```

4) Save the policy template.
5) Refresh the policies of all firewalls involved in the VPN to activate the new configuration.

Add rule to allow traffic without encryption or decryption

See section *Create a Firewall Policy* in this guide for detailed steps.

- For the field **Use Action** set it to **Allow option without any VPN Action** option to allow traffic without encryption or decryption.

Add rules to deny traffic as needed

See section *Create a Firewall Policy* in this guide for detailed steps.

- For the field **Use Action** set it to **Discard** option to deny traffic.

Enabling communication between the SMC and NGFW Engine

The target of evaluation uses a registration process to join NGFW Engines to the SMC using a registration channel. The administrator enables the NGFW Engine joining by saving the initial configuration in the SMC before the registration channel is established. The SMC generates a one-time password that is used as a secret in enabling process. The administrator has to take note of the one-time password and enter it on the NGFW Engine console to initiate the registration process. The NGFW Engine initiates the communication to set up the registration channel.

Preparations for the registration

- Prepare the configuration as described in section, *Preparations for the configuration*.
- Make sure that the Virtual SMC Appliance is installed in FIPS mode using 256-bit security setting according to Enable FIPS mode on the SMC Appliance.
- Make sure that the joining NGFW Engine is installed in FIPS mode using the 256-bit security setting according to Install the NGFW Engine in FIPS mode.
- Verify that the Virtual SMC is connected to the management network using its management network interface.
- Verify that the joining NGFW Engine is connected to the management network using its management network interface.

The SMC and NGFW Engines use TLS for protected communications and X.509 certificates for mutual authentication.

When the SMC is installed, an internal ECDSA certificate authority is automatically created. The internal certificate authority issues certificates for the SMC components during the virtual SMC Appliance installation. NGFW Engine certificates are issued during the registration process.

A secure TLS communication channel is established for the registration. The administrator confirms or enters the expected SMC certificate SHA-512 hash for authentication. SMC authenticates the NGFW Engine using an SMC generated one-time password that the administrator inputs into the NGFW Engine.

During the registration process SMC sends the internal CA certificate to the NGFW Engine, the NGFW Engine generates a certificate signing request, the SMC internal CA issues a certificate that the SMC sends to the NGFW Engine, and the NGFW Engine validates the received certificate.

In the 256-bit mode ECDSA P-521 with SHA-512 digital signatures is used in all certificates for the communication between SMC and NGFW Engines. The reference identifiers in the SAN DNS field for subsequent TLS client and server authentication are configured automatically during the registration.

After initial contact is made, subsequent TLS connections between the components are mutually authenticated.

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 140-3 mode and enable 256-bit encryption as the security strength when you install the NGFW Engine.

256-bit encryption with the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS cipher suite is used for the connection between the NGFW Engine and the Management Server. 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

Note

With current release, FIPS 140-3 standard is supported.

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**.

6) 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

1) Select **Configuration**.

2) Right-click the NGFW Engine, then select **Commands** > **Reset to Factory Settings**.

3) In the **Number of Overwrites** field, enter how many times you want the stored data on the file system to be overwritten.

4) If you want the appliance to turn off after the factory reset has completed, select **Shut Down After Reset**.

5) Click **OK**.

6) 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 NGFW 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.
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.

Note

The SenderType field contains "Management Server", "Log Server", or "Firewall" for Management Server, Log Server, and NGFW Engine, respectively, and the NodeId contains the IP address of the sender. The SMC Appliance syslogs are sent from a loopback address and include the hostname of the Virtual SMC Appliance after the timestamp of the syslog message.

FAU_GEN.1.1 a)	
Auditable event	Start up and shutdown of the audit functions.
Startup of SMC Appliance	`Apr 7 11:56:44 192.0.2.2 Timestamp="2021-04-07 11:56:44", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353012225", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.start", Result="Success", ObjectName="Audit function started"`  `Apr 9 10:14:48 192.0.2.2 Timestamp="2021-04-09 10:14:48", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", SenderType="Log Server", EventId="3977579151379922945", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.start", Result="Success", ObjectName="Audit function started"`
Shutdown of SMC Appliance	`Apr 7 11:52:30 192.0.2.2 Timestamp="2021-04-07 11:52:30", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3248529000007467185", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.stop", Result="Success", ObjectName="Audit function shutdown"`  `Apr 7 12:56:45 192.0.2.2 Timestamp="2021-04-07 12:56:45", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", SenderType="Log Server", EventId="3261934555010958085", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.stop", Result="Success", ObjectName="Audit function shutdown"`

FAU_GEN.1.1 a)	
Startup of NGFW Engine	Apr 6 18:57:16 192.0.2.4 Timestamp="2021-04-06 18:57:16", LogId="1047478", NodeId="192.0.2.4", Facility="System Utilities", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="Auditing log start", ReceptionTime="2021-04-06 18:57:16", SenderType="Firewall", SituationId="78022", Situation="System_Engine-Log-Auditing-State", EventId="6785228912345480118"
Shutdown of NGFW Engine	Apr 6 18:56:14 192.0.2.4 Timestamp="2021-04-06 18:56:14", LogId="1047463", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="Auditing log end", ReceptionTime="2021-04-06 18:57:16", SenderType="Firewall", SituationId="78022", Situation="System_Engine-Log-Auditing-State", EventId="6785228654647442343"

FAU_GEN.1.1 c)	
Auditable event	Administrative login and logout
Administrative login	Apr 7 16:59:50 192.0.2.2 Timestamp="2021-04-07 16:59:50", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login succeeded for user test00 in domain Shared Domain", SenderType="Management Server", EventId="3261674911353013518", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.login", Result="Success", ObjectName="test00;Shared Domain"
Administrative logout	Apr 7 16:56:43 192.0.2.2 Timestamp="2021-04-07 16:56:43", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Logout succeeded for user test00.", SenderType="Management Server", EventId="3261674911353013508", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.logout", Result="Success", ObjectName="test00"

FMT_SMF.1, FAU_GEN.1.1 c)	
Auditable event	Security related configuration changes
Audit server configuration changes	Apr 7 14:19:54 192.0.2.2 Timestamp="2021-04-07 14:19:54", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A new log forward rule was created with All Log Data types to host Syslog (port 6514).", SenderType="Management Server", EventId="3261674911353012817", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.log.forward.new", Result="Success", ObjectName="LogServer 192.0.2.2" Apr 7 14:20:06 192.0.2.2 Timestamp="2021-04-07 14:20:06", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A log forward rule was deleted.", SenderType="Management Server", EventId="3261674911353012827", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.log.forward.deleted", Result="Success", ObjectName="LogServer 192.0.2.2"
Configuring reference identifier for the peer	Aug 12 07:22:55 10.0.23.186 Timestamp="2021-08-12 07:22:55", NodeId="10.0.23.186", CompId="Management Server", InfoMsg="netflow_collector has been added: <netflow_collector data_context='Audit' netflow_collector_host_ref='syslog-tls' netflow_collector_port='2055' netflow_collector_service='tcp_with_tls' netflow_collector_version='esm' tls_identity='DNS Name / syslog-tls.example.com' tls_profile='syslog-tls-profile'/>.", SenderType="Management Server", EventId="6023801935990112299", UserOriginator="test00", ClientIpAddress="10.0.23.248", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Management Server"

FMT_SMF.1, FAU_GEN.1.1 c)	
Modification of administrator accounts	Apr 7 15:15:56 192.0.2.2 Timestamp="2021-04-07 15:15:56", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353013069", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="admin2" Apr 7 15:16:28 192.0.2.2 Timestamp="2021-04-07 15:16:28", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353013075", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.disabled", Result="Success", ObjectName="admin2" Apr 7 17:34:30 192.0.2.2 Timestamp="2021-04-07 17:34:30", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353013648", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.enabled", Result="Success", ObjectName="admin2"
Logon banner change	Apr 7 17:35:33 192.0.2.2 Timestamp="2021-04-07 17:35:33", 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="3261674911353013656", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.update", Result="Success", ObjectName="logon_banner_text"
Minimum password length	Apr 7 17:35:33 192.0.2.2 Timestamp="2021-04-07 17:35:33", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Updated Global System Property password_character_number_minimum to 10", SenderType="Management Server", EventId="3261674911353013655", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.update", Result="Success", ObjectName="password_character_number_minimum"

FMT_SMF.1, FAU_GEN.1.1 c)	

Remote session timeout change	<pre>Sep 29 14:50:40 192.0.2.2 Timestamp="2021-09-29 14:50:40",
	NodeId="192.0.2.2",
	CompId="Management Server",
	InfoMsg="Updated Global System Property gui_inactivity_max_in_min to 5",
	SenderType="Management Server",
	EventId="3485048704354747658",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.update",
	Result="Success",
	ObjectName="gui_inactivity_max_in_min"</pre>
	<pre>Sep 29 14:50:40 192.0.2.2 Timestamp="2021-09-29 14:50:40",
	NodeId="192.0.2.2",
	CompId="Management Server",
	InfoMsg="Updated Global System Property behavior_after_reach_gui_inactivity_max
	to TERMINATE_SESSION",
	SenderType="Management Server",
	EventId="3485048704354747659",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.update",
	Result="Success",
	ObjectName="behavior_after_reach_gui_inactivity_max"</pre>
	<pre>Sep 29 15:33:32 127.0.0.1 Timestamp="2021-09-29 15:33:32",
	NodeId="127.0.0.1",
	Type="Notification",
	CompId="3",
	InfoMsg="Sep 29 15:33:32 smca admin: changed console timeout to 300",
	ReceptionTime="2021-09-29 15:33:32",
	SenderType="Third Party Device",
	EventId="13120"</pre>

Configure authentication failure parameters for FIA_AFL.1	<pre>Sep 29 17:09:23 192.0.2.2 Timestamp="2021-09-29 17:09:23",
	NodeId="192.0.2.2",
	CompId="Management Server",InfoMsg="Updated Global System Property
	conf_time_login_delayed to 1",
	SenderType="Management Server",
	EventId="3485048704354747989",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.update",
	Result="Success",
	ObjectName="conf_time_login_delayed"</pre>
	<pre>Sep 29 17:09:23 192.0.2.2 Timestamp="2021-09-29 17:09:23",
	NodeId="192.0.2.2",
	CompId="Management Server",
	InfoMsg="Updated Global System Property failed_auth_attempt_before_delay to 3",
	SenderType="Management Server",
	EventId="3485048704354747988",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.update",
	Result="Success",ObjectName="failed_auth_attempt_before_delay"</pre>

Auditable event	Configuration of time

FMT_SMF.1, FAU_GEN.1.1 c)	

Configuration of a new time server	<pre>Aug 12 07:12:34 10.0.23.186 Timestamp="2021-08-12 07:12:34",
	NodeId="10.0.23.186",
	CompId="Management Server",
	InfoMsg="ntp_server element has been created.",
	SenderType="Management Server",
	EventId="6023801935990112251",
	UserOriginator=" test00",
	ClientIpAddress="10.0.23.248",
	TypeDescription="stonegate.object.insert",
	Result="Success",
	ObjectName="myntpserver"</pre>

Auditable event	Configuration of the cryptographic functionality

Configure the cryptographic functionality for TLS	<pre>Sep 29 18:44:17 192.0.2.2 Timestamp="2021-09-29 18:44:17",
	NodeId="192.0.2.2",
	CompId="Management Server",
	InfoMsg="tls_cryptography_suite_set element has been created.",
	SenderType="Management Server",
	EventId="3485048704354748131",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.insert",
	Result="Success",
	ObjectName="TLS Suites"</pre>
	<pre>Sep 29 18:45:11 192.0.2.2 Timestamp="2021-09-29 18:45:11",
	NodeId="192.0.2.2",
	CompId="Management Server",
	InfoMsg="tls_cryptography_suites has been modified on its attribute:
	tls_rsa_with_aes_128_cbc_sha (true -> false).",
	SenderType="Management Server",
	EventId="3485048704354748135",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.update.details",
	Result="Success",
	ObjectName="TLS Suites"</pre>
	<pre>Sep 29 18:48:21 192.0.2.2 Timestamp="2021-09-29 18:48:21",
	NodeId="192.0.2.2",
	CompId="Management Server",
	SenderType="Management Server",
	EventId="3485048704354748156",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.update",
	Result="Success",
	ObjectName="Management Server"</pre>

FMT_SMF.1, FAU_GEN.1.1 c)	
Configure the cryptographic functionality for TLS (continued)	Sep 29 18:48:21 192.0.2.2 Timestamp="2021-09-29 18:48:21", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="web_app (webswing) has been modified on its attribute: tls_cipher_suites (NIST (SP 800-52 Rev. 2) Compatible TLS Cryptographic Algorithms -> TLS Suites).", SenderType="Management Server", EventId="3485048704354748153", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Management Server" Sep 29 18:55:48 192.0.2.2 Timestamp="2021-09-29 18:55:48", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="tls_cryptography_suite_set_ref has been modified (NIST (SP 800-52 Rev. 2) Compatible TLS Cryptographic Algorithms -> TLS Suites).", SenderType="Management Server", EventId="3485048704354748172", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Audit TLS" Sep 29 18:55:48 192.0.2.2 Timestamp="2021-09-29 18:55:48", NodeId="192.0.2.2",CompId="Management Server", SenderType="Management Server", EventId="3485048704354748173", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update" ,Result="Success", ObjectName="Audit TLS"

FMT_SMF.1, FAU_GEN.1.1 c)	

Configure the cryptographic functionality for TLS (continued)	<pre>Sep 29 18:59:53 192.0.2.2 Timestamp="2021-09-29 18:59:53",
	NodeId="192.0.2.2",
	CompId="Management Server",
	InfoMsg="netflow_collector has been modified on its attribute: tls_profile (No
	 value -> Audit TLS).",
	SenderType="Management Server",
	EventId="3485048704354748184",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.update.details",
	Result="Success",
	ObjectName="Management Server"</pre>
	<pre>Sep 29 18:59:53 192.0.2.2 Timestamp="2021-09-29 18:59:53",
	NodeId="192.0.2.2",
	CompId="Management Server",
	InfoMsg="netflow_collector has been modified on its attribute:
	 netflow_collector_service (tcp -> tcp_with_tls).",
	SenderType="Management Server",
	EventId="3485048704354748185",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.update.details",
	Result="Success",
	ObjectName="Management Server"</pre>

Configure the cryptographic functionality for NTP (continued)	<pre>Sep 29 19:08:49 192.0.2.2 Timestamp="2021-09-29 19:08:49",
	NodeId="192.0.2.2",
	CompId="Management Server",
	InfoMsg="ntp_auth_key_type has been modified (none -> SHA1).",
	SenderType="Management Server",
	EventId="3485048704354748268",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.update.details",
	Result="Success",
	ObjectName="NTP server"</pre>
	<pre>Sep 29 19:08:49 192.0.2.2 Timestamp="2021-09-29 19:08:49",
	NodeId="192.0.2.2",
	CompId="Management Server",
	SenderType="Management Server",
	EventId="3485048704354748269",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.update",
	Result="Success",
	ObjectName="NTP server"</pre>

Auditable event	Generating / import of, changing, or deleting of cryptographic keys

FMT_SMF.1, FAU_GEN.1.1 c)	
Creation of a TLS private key (**Configuration** > **Administration** > **Certificates** > **TLS Credentials** > **New TLS Credentials**)	`Apr 7 17:13:43 192.0.2.2 Timestamp="2021-04-07 17:13:43", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Cryptographic key generated", SenderType="Management Server", EventId="3261674911353013583", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.cryptographic_key.new", Result="Success", ObjectName="Audit TLS Key"`
Certificate signing request	`Apr 7 17:16:48 192.0.2.2 Timestamp="2021-04-07 17:16:48", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Credentials certificate signing request was exported. The fingerprint is 7B:19:28:F7:64:CA:84:34:31:7F:F6:C5:14:B2:D8:36:00:8E:A9:44.", SenderType="Management Server", EventId="3339846631854964740", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.certificate.export", Result="Success", ObjectName="Audit TLS CSR"`
Import signed certificate	`Apr 7 17:19:15 192.0.2.2 Timestamp="2021-04-07 17:19:15", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353013605", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.certificate.import", Result="Success", ObjectName="Audit CSR import cert"`
Deletion (from Trash)	`Apr 7 17:10:53 192.0.2.2 Timestamp="2021-04-07 17:10:53", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353013566", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.cryptographic_key.deleted", Result="Success", ObjectName="Audit TLS Key"`

FMT_SMF.1, FAU_GEN.1.1 c)	
Import of a trusted certificate authority (CA)	Apr 7 17:18:30 192.0.2.2 Timestamp="2021-04-07 17:18:30", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="tls_certificate_authority element has been created.", SenderType="Management Server", EventId="3261674911353013603", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="Audit Trusted CA" Apr 7 17:18:30 192.0.2.2 Timestamp="2021-04-07 17:18:30", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A local certificate key was imported into a Trusted Certificate Authority.", SenderType="Management Server", EventId="3339846631854964743", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.certificate.import", Result="Success", ObjectName="Audit Trusted CA"
Import of a private key and a certificate	Apr 7 17:09:10 192.0.2.2 Timestamp="2021-04-07 17:09:10", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353013559", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.certificate.import", Result="Success", ObjectName="Audit Key" Apr 7 17:09:10 192.0.2.2 Timestamp="2021-04-07 17:09:10", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Cryptographic key imported", SenderType="Management Server", EventId="3261674911353013558", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.cryptographic_key.import", Result="Success", ObjectName="Audit Key" Apr 7 17:09:10 192.0.2.2 Timestamp="2021-04-07 17:09:10", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353013560", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="Audit Key"

FMT_SMF.1, FAU_GEN.1.1 c)	

Removal (Deletion) of a Trusted Certificate Authority	<pre>Sep 29 19:35:06 192.0.2.2 Timestamp="2021-09-29 19:35:06",
	NodeId="192.0.2.2",
	CompId="Management Server",
	SenderType="Management Server",
	EventId="3485048704354748418",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.cryptographic_key.deleted",
	Result="Success",ObjectName="Trusted Root CA"</pre><pre>Sep 29 19:35:06 192.0.2.2 Timestamp="2021-09-29 19:35:06",
	NodeId="192.0.2.2",
	CompId="Management Server",
	SenderType="Management Server",
	EventId="3485048704354748417",
	UserOriginator="admin",
	ClientIpAddress="192.0.2.1",
	TypeDescription="stonegate.object.delete",
	Result="Success",
	ObjectName="Trusted Root CA"</pre>

Auditable event	Resetting passwords

Password reset	<pre>Apr 7 17:36:13 192.0.2.2 Timestamp="2021-04-07 17:36:13",
	NodeId="192.0.2.2",
	CompId="Management Server",
	SenderType="Management Server",
	EventId="3261674911353013659",
	UserOriginator="test00",
	ClientIpAddress="192.0.2.11",
	TypeDescription="stonegate.admin.password.change",
	Result="Success",
	ObjectName="admin2"</pre>

FCS_NTP_EXT.1, FAU_GEN.1.1 c)	
Configuration of a new time server (continued)	2021-09-19T22:51:07.488895-04:00 smc1000 "2021-09-19 21:47:42", "7687275677770322937", "172.16.16.240", "Management Server",, "test00", "172.16.16.253", "stonegate.object.update.details", "Success", "N60", "ntp_settings has been modified on its attribute: ntp_preferred_server_ref (No value -> tl7-16x).",, "Management Server" 2021-09-19T22:51:07.489600-04:00 smc1000 "2021-09-19 21:47:42", "7687275677770322939", "172.16.16.240", "Management Server",, "test00", "172.16.16.253", "stonegate.object.update.details", "Success", "N60", "ntp_server_ref has been added: <ntp_server_ref ref=\"tl7-16x\"/>.",, "Management Server"
Removal of configured time server	Aug 12 07:15:36 10.0.23.186 Timestamp="2021-08-12 07:15:36", NodeId="10.0.23.186", CompId="Management Server", SenderType="Management Server", EventId="6023801935990112259", UserOriginator="test00", ClientIpAddress="10.0.23.248", TypeDescription="stonegate.object.delete", Result="Success", ObjectName="myntpserver" 2021-09-19T23:02:59.589828-04:00 smc1000 "2021-09-19 21:59:34", "7687275677770322950", "172.16.16.240", "Management Server",, "test00", "172.16.16.253", "stonegate.object.update.details", "Success", "N60", "ntp_settings has been modified on its attribute: ntp_preferred_server_ref (tl7-16x -> No value).",, "Management Server" 2021-09-19T23:02:59.589828-04:00 smc1000 "2021-09-19 21:59:34", "7687275677770322952", "172.16.16.240", "Management Server",, "test00", "172.16.16.253", "stonegate.object.update.details", "Success", "N60", "ntp_server_ref has been removed: <ntp_server_ref ref=\"tl7-16x\"/>.",, "Management Server"

FCS_NTP_EXT.1, FAU_GEN.1.1 c)	
Manual time change	Mar 31 17:28:01 192.0.2.2 : :1 Timestamp="2021-03-31 17:28:01", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Mar 31 17:28:01 smca0 sudo: test00 : TTY=pts/0 ; PWD=/home/test00 ; USER=root ; COMMAND=/bin/date -s Wed Mar 31 17:28:10 CDT 2021", ReceptionTime="2021-03-31 17:28:01", SenderType="Third Party Device", EventId="35810"

FMT SMF.1/FFW FAU_GEN.1.1 c)	
Firewall filtering rule change	Apr 7 17:23:02 192.0.2.2 Timestamp="2021-04-07 17:23:02", NodeId="192.0.2.2", RuleId="106.8", CompId="Management Server", InfoMsg="IPv4 Access Rule @106.8 has been modified.", SenderType="Management Server", EventId="3261674911353013615", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.update", Result="Success", ObjectName="anypolicy"
Firewall security policy change	Apr 7 17:23:02 192.0.2.2 Timestamp="2021-04-07 17:23:02", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353013618", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.update", Result="Success", ObjectName="anypolicy" Apr 7 13:57:39 192.0.2.2 Timestamp="2021-04-07 13:57:39", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353012582", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.policy.upload.start", Result="Success", ObjectName="anypolicy;NGFW"

FMT SMF.1/FFW FAU_GEN.1.1 c)	
Firewall security policy change (continued)	Apr 7 13:57:52 192.0.2.2 Timestamp="2021-04-07 13:57:52", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353012587", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.firewall.policy.upload", Result="Success", ObjectName="NGFW;anypolicy" Apr 7 13:57:52 192.0.2.2 Timestamp="2021-04-07 13:57:52", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353012588", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.policy.upload.end", Result="Success", ObjectName="anypolicy;NGFW"
Firewall security policy change (add rule)	Sep 29 19:47:44 192.0.2.2 Timestamp="2021-09-29 19:47:44", NodeId="192.0.2.2", RuleId="2097155.0", CompId="Management Server", InfoMsg="IPv4 Access Rule @2097155.0 has been added.", SenderType="Management Server", EventId="3485048704354748467", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="Firewall Policy" Sep 29 19:47:45 192.0.2.2 Timestamp="2021-09-29 19:47:45", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="access_entry has been added: <rule_entry comment='Ping' is_disabled='false' parent_rule_ref='Access rule : insert point' rank='1.0' tag='2097155.0'> <match_part> <match_sources> <match_source_ref type='network_element' value='network-198.51.100.0/24'/> </match_sources> <match_destinations> <match_destination_ref type='network_element' value='network-203.0.113.0/24'/></match_destinations> <match_services> <match_service_ref type='service' value='Ping'/> </match_services> </ match_part> <option> <log_policy closing_mode='true' log_level='undefined' mss_enforce='false'/> </option> </rule_entry>.", SenderType="Management Server", EventId="3485048704354748468", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Firewall Policy"

FMT SMF.1/FFW FAU_GEN.1.1 c)	
Firewall security policy change (delete rule)	Sep 29 19:48:00 192.0.2.2 Timestamp="2021-09-29 19:48:00", NodeId="192.0.2.2", RuleId="2097155.0", CompId="Management Server", InfoMsg="IPv4 Access Rule @2097155.0 has been deleted.", SenderType="Management Server", EventId="3485048704354748473", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.delete", Result="Success", ObjectName="Firewall Policy" Sep 29 19:48:00 192.0.2.2 Timestamp="2021-09-29 19:48:00", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="rule_entry has been removed: <rule_entry comment='Ping' is_disabled='false' parent_rule_ref='Access rule : insert point' rank='1.0' rule_tag_major_id='2097155' tag='2097155.0'> <match_part> <match_sources> <match_source_ref type='network_element' value='network-198.51.100.0/24'/> </ match_sources> <match_destinations> <match_destination_ref type='network_element' value='network-203.0.113.0/24'/> </match_destinations> <match_services> <match_service_ref type='service' value='Ping'/> </match_services> </ match_part> <option> <log_policy closing_mode='true' log_level='undefined' mss_enforce='false'/> </option> </rule_entry>.", SenderType="Management Server", EventId="3485048704354748474", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Firewall Policy"
Firewall security policy change (create policy)	Sep 29 19:46:14 192.0.2.2 Timestamp="2021-09-29 19:46:14", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="fw_policy element has been created.", SenderType="Management Server", EventId="3485048704354748466", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="Firewall Policy"

FMT SMF.1/FFW FAU_GEN.1.1 c)	
Firewall security policy change (upload policy)	Sep 29 19:55:20 192.0.2.2 Timestamp="2021-09-29 19:55:20", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3485048704354748507", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.policy.upload.start", Result="Success",ObjectName="Firewall Policy;NGFW" Sep 29 19:55:26 192.0.2.2 Timestamp="2021-09-29 19:55:26",NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3485048704354748510", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.firewall.policy.upload", Result="Success", ObjectName="NGFW;Firewall Policy" Sep 29 19:55:26 192.0.2.2 Timestamp="2021-09-29 19:55:26", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3485048704354748511", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.policy.upload.end", Result="Success", ObjectName="Firewall Policy;NGFW"
Firewall security policy change (delete policy)	Sep 29 20:06:05 192.0.2.2 Timestamp="2021-09-29 20:06:05", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3485048704354748572", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.trash.add", Result="Success", ObjectName="Firewall Policy" Sep 29 20:06:12 192.0.2.2 Timestamp="2021-09-29 20:06:12", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3485048704354748573", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.delete", Result="Success", ObjectName="Firewall Policy"

FMT_SMF.1/VPN, FAU_GEN.1.1 c) VPN security policy change	
VPN security policy change (adding rule)	Apr 5 13:30:46 192.0.2.2 Timestamp="2023-04-05 13:30:46", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="rule_entry has been added: <rule_entry is_disabled='false' parent_rule_ref='Access rule : insert point' rank='1.5' rule_tag_major_id='2097201' tag='2097201.0'><match_part><match_sources><match_source_ref type='network_element' value='network-198.51.100.0/24'/></ match_sources><match_destinations><match_destination_ref type='network_element' value='network-10.0.51.0/24'/></ match_destinations><match_services><match_service_ref type='service' value='ANY'/></match_services></match_part><vpn_action meta_mobile_vpn='false' type='enforce'><vpn_ref ref='Test VPN'/></vpn_action><option><log_policy closing_mode='true' log_level='undefined' mss_enforce='false'/></option></ rule_entry>.", SenderType="Management Server", EventId="5830093877238825026", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Site-to-site VPN"
VPN security policy change (modify rule)	Apr 5 13:33:08 192.0.2.2 Timestamp="2023-04-05 13:33:08", NodeId="192.0.2.2", RuleId="2097201.3", CompId="Management Server", InfoMsg="IPv4 Access Rule @2097201.3 has been modified.", SenderType="Management Server", EventId="5830093877238825036", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="Site-to-site VPN" Apr 5 13:33:09 192.0.2.2 Timestamp="2023-04-05 13:33:09", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="match_source_ref has been added: <match_source_ref type='network_element' value='network-192.0.2.0/24'/>.", SenderType="Management Server", EventId="5830093877238825037", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Site-to-site VPN"

FMT_SMF.1/VPN, FAU_GEN.1.1 c) VPN security policy change	
VPN security policy change (delete rule)	Apr 5 13:34:05 192.0.2.2 Timestamp="2023-04-05 13:34:05", NodeId="192.0.2.2", RuleId="2097201.3", CompId="Management Server", InfoMsg="IPv4 Access Rule @2097201.3 has been deleted.", SenderType="Management Server", EventId="5830093877238825039", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.delete", Result="Success", ObjectName="Site-to-site VPN" Apr 5 13:34:05 192.0.2.2 Timestamp="2023-04-05 13:34:05", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="rule_entry has been removed: <rule_entry is_disabled='false' parent_rule_ref='Access rule : insert point' rank='1.5' rule_tag_major_id='2097201' tag='2097201.3'><match_part><match_sources><match_source_ref type='network_element' value='network-192.0.2.0/24'/><match_source_ref type='network_element' value='network-198.51.100.0/24'/></ match_sources><match_destinations><match_destination_ref type='network_element' value='network-10.0.51.0/24'/></ match_destinations><match_services><match_service_ref type='service' value='ANY'/></match_services></match_part><vpn_action meta_mobile_vpn='false' type='enforce'><vpn_ref ref='Test VPN'/></vpn_action><option><log_policy log_compression='off' log_level='undefined' mss_enforce='false'/></option></ rule_entry>.", SenderType="Management Server", EventId="5830093877238825040", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Site-to-site VPN"

FPT_STM_EXT.1	
NTP time change	May 6 13:40:40 192.0.2.2 : :1 Timestamp="2021-05-06 13:40:40", NodeId="::1", Type="Notification", CompId="3", InfoMsg="May 6 13:40:40 smca0 chronyd[32473]: Backward time jump detected! Before: 2021-05-06 18:47:55 After: 2021-05-06 18:40:40", ReceptionTime="2021-05-06 13:40:40", SenderType="Third Party Device", EventId="34667" May 6 13:48:32 192.0.2.2 : :1 Timestamp="2021-05-06 13:48:32", NodeId="::1", Type="Notification", CompId="3", InfoMsg="May 6 13:48:32 smca0 chronyd[32473]: System clock was stepped by 453.764139 seconds", ReceptionTime="2021-05-06 13:48:32", SenderType="Third Party Device", EventId="34703" May 6 13:54:40 192.0.2.2 : :1 Timestamp="2021-05-06 13:54:40", NodeId="::1", Type="Notification", CompId="3", InfoMsg="May 6 13:54:40 smca0 chronyd[32473]: Forward time jump detected! Before: 2021-05-06 18:49:28 After: 2021-05-06 18:54:40", ReceptionTime="2021-05-06 13:54:40", SenderType="Third Party Device", EventId="35062"
NTP time change (continued)	May 6 13:50:35 192.0.2.2 : :1 Timestamp="2021-05-06 13:50:35", NodeId="::1", Type="Notification", CompId="3", InfoMsg="May 6 13:50:35 smca0 chronyd[32473]: System clock was stepped by -261.671263 seconds", ReceptionTime="2021-05-06 13:50:35", SenderType="Third Party Device", EventId="35107" Apr 29 16:12:33 192.0.2.4 Timestamp="2021-04-29 16:12:33", LogId="4218", NodeId="192.0.2.4", Facility="Syslog", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="ntpd: Time change. Before: Thu Apr 29 16:11:33 After: Thu Apr 29 16:12:33 Peer: 192.0.2.10", ReceptionTime="2021-04-29 16:11:33", SenderType="Firewall", EventId="6793522378228895866"

FCS_TLSC_EXT.1	
Auditable event	TLS client sessions

FCS_TLSC_EXT.1	
Failure to establish a TLS client session	Apr 7 16:05:39 192.0.2.2 Timestamp="2021-04-07 16:05:39", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.10 port=6514] Local = [port=54854] Syslog authentication failed. [192.0.2.10:6514] Details: Received fatal alert: handshake_failure", SenderType="Management Server", EventId="3261674911353013303", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"

FCS_TLSS_EXT.1,FCS_HTTPS_EXT.1,FTP_TRP.1/Admin	
Auditable event	HTTPS and TLS sessions, and trusted path
Initiation of an HTTPS or TLS session, or trusted path	Sep 29 13:06:14 192.0.2.2 Timestamp="2021-09-29 13:06:14", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.100 port=43054] Local = [host=192.0.2.2 port=8085]", SenderType="Management Server", EventId="3485048704354747192", UserOriginator="System", ClientIpAddress="192.0.2.100", TypeDescription="stonegate.trusted.connection.start", Result="Success"
Termination of an HTTPS or TLS session, or trusted path	Sep 29 13:10:22 192.0.2.2 Timestamp="2021-09-29 13:10:22", NodeId="192.0.2.2",CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.100 port=43054] Local = [host=192.0.2.2 port=8085]", SenderType="Management Server", EventId="3485048704354747241", UserOriginator="System", ClientIpAddress="192.0.2.100", TypeDescription="stonegate.trusted.connection.end", Result="Success"
Failure to establish an HTTPS or TLS session, or trusted path	Sep 29 13:21:18 192.0.2.2 Timestamp="2021-09-29 13:21:18", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.100 port=43068] Local = [host=192.0.2.2 port=8085] ERROR: no cipher suites in common", SenderType="Management Server", EventId="3485048704354747 256", UserOriginator="System", ClientIpAddress="192.0.2.100", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"

FCS_TLSS_EXT.2	
Auditable event	TLS sessions

FCS_TLSS_EXT.2	
Failure to authenticate the client (SMC as a server)	Jan 11 13:05:40 192.0.2.2 Timestamp="2023-01-11 13:05:40", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.4 port=34784] Local = [port=3020] ERROR: Communication authentication failed. [192.0.2.4:34784] Details: Empty server certificate chain", SenderType="Log Server", EventId="2340561922811756578", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"
Failure to authenticate the client (NGFW Engine as a server)	Sep 29 11:10:17 192.0.2.4 Timestamp="2021-09-29 11:10:17", LogId="711", NodeId="192.0.2.4", Facility="Management", Type="Error", CompId="NGFW node 1", InfoMsg="peer did not return a certificate", ReceptionTime="2021-09-29 11:10:17", SenderType="Firewall", SituationId="9005", Situation="FW_Communication-Communication-Error", EventId="6848891653499912903" Sep 29 11:10:17 192.0.2.4 Timestamp="2021-09-29 11:10:17", LogId="712", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW node 1", InfoMsg="TLS: Couldn't accept TLS connection (3 192.0.2.2)", ReceptionTime="2021-09-29 11:10:17", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6848891653499912904"

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	May 20 14:56:55 172.20.120.60 Timestamp="2021-05-20 14:56:55", LogId="219", NodeId="172.20.120.60", Facility="System Utilities", Type="Notification", Srcif="6", CompId="120-FIPS node 1", ReceptionTime="2021-05-20 14:56:56", SenderType="Firewall", SituationId="78023", Situation="System_Engine-NIC-Dropped-RX-Packets", EventId="6801113488111435995"

FFW_RUL_EXT.1	
Half-open connection limit	Apr 7 13:42:10 192.0.2.4 Timestamp="2021-04-07 13:42:10", LogId="1049269", 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="2021-04-07 13:42:10", SenderType="Firewall", SituationId="79990", Situation="DOS_SYN-Flood-Started", EventId="6785511997933880805"
Auditable event	Application of rules configured with the 'log' operation
Connection allowed	Apr 4 10:35:51 192.0.2.4 Timestamp="2023-04-04 10:35:51", LogId="514333", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="New connection", Action="Allow",Protocol="6", Src="198.51.100.100", Dst="203.0.113.100", Sport="60290", Dport="80", RuleId="2097195.1", Srcif="1", CompId="NGFW node 1", ReceptionTime="2023-04-04 10:35:51", SenderType="Firewall", SituationId="70018", Situation="Connection_Allowed", EventId="7048921092362076452", Service="HTTP
Connection discarded	Apr 4 10:21:05 192.0.2.4 Timestamp="2023-04-04 10:21:05", LogId="513964", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="Connection discarded", Action="Discard",Protocol="6", Src="203.0.113.100", Dst="198.51.100.100", Sport="53098", Dport="80", RuleId="2097171.0", Srcif="2", CompId="NGFW node 1", ReceptionTime="2023-04-04 10:21:06", SenderType="Firewall", SituationId="70019", Situation="Connection_Discarded", EventId="7048917377215365298", Service="HTTP"

FFW_RUL_EXT.2	
Auditable event	Dynamical definition of rule and establishment of a session

Dynamical definition of rule and establishment of a session	<pre>Sep 29 14:32:51 192.0.2.4 Timestamp="2021-09-29 14:32:51",
	LogId="1490",
	NodeId="192.0.2.4",
	Facility="Packet Filtering",
	Type="Notification",
	Event="New connection",
	Action="Allow",
	Protocol="6",
	Src="198.51.100.100",
	Dst="203.0.113.100",
	Sport="55516",
	Dport="21",
	RuleId="2097154.0",
	Srcif="1",
	CompId="NGFW node 1",
	ReceptionTime="2021-09-29 14:32:51",
	SenderType="Firewall",
	SituationId="70018",
	Situation="Connection_Allowed",
	EventId="6848942630466749122",
	Service="FTP"</pre>
	<pre>Sep 29 14:32:57 192.0.2.4 Timestamp="2021-09-29 14:32:57",
	LogId="1491",
	NodeId="192.0.2.4",
	Facility="Packet Filtering",
	Type="Notification",
	Event="Related connection",
	Action="Allow",
	Protocol="6",
	Src="203.0.113.100",
	Dst="198.51.100.100",
	Sport="20",
	Dport="57585",
	RuleId="2097154.0",
	Srcif="2;2",
	CompId="NGFW node 1",
	ReceptionTime="2021-09-29 14:32:57",
	SenderType="Firewall",SituationId="1004",
	Situation="FW_Related-Connection",
	EventId="6848942656236552899",
	Service="TCP/57585"</pre>

FIA_AFL.1	
Auditable event	Unsuccessful login attempt limit is met or exceeded

FIA_AFL.1	
Prevent the offending remote Administrator from successfully authenticating until an Administrator defined time period has elapsed	Apr 8 14:41:54 192.0.2.2 Timestamp="2021-04-08 14:41:54", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Too many login failures wait 30 min minutes to retry. ERROR: Authentication failed. The user name or password might be incorrect. Verify that the address of the server is correct and that it is running properly. ", SenderType="Management server", EventId="3261674911353015028", UserOriginator="System", ClientIpAddress="10.21.161.1", TypeDescription="stonegate.admin.login", Result="Fail", ObjectName="admin1"

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Auditable event	All use of identification and authentication mechanism
Local session identification and authentication failures	Apr 6 15:40:43 192.0.2.2 : :1 Timestamp="2021-04-06 15:40:43", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:40:43 smca0 login: pam_unix(login:auth): check pass; user unknown", ReceptionTime="2021-04-06 15:40:43", SenderType="Third Party Device", EventId="116147" Apr 6 15:40:43 192.0.2.2 : :1 Timestamp="2021-04-06 15:40:43", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:40:43 smca0 login: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost=", ReceptionTime="2021-04-06 15:40:43", SenderType="Third Party Device", EventId="116148"
Local session identification and authentication failures (continued)	Apr 6 15:40:43 192.0.2.2 : :1 Timestamp="2021-04-06 15:40:43", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:40:43 smca0 login: pam_faillock(login:auth): User unknown", ReceptionTime="2021-04-06 15:40:43", SenderType="Third Party Device", EventId="116149" Apr 6 15:46:56 192.0.2.2 : :1 Timestamp="2021-04-06 15:46:56", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:46:56 smca0 login: FAILED LOGIN SESSION FROM tty1 FOR admin1 Permission denied", ReceptionTime="2021-04-06 15:46:56", SenderType="Third Party Device", EventId="116975"

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Local session identification and authentication failures (continued)	Apr 6 15:46:54 192.0.2.2 : :1 Timestamp="2021-04-06 15:46:54", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:46:54 smca0 unix_chkpwd[533861]: password check failed for user (admin1)", ReceptionTime="2021-04-06 15:46:54", SenderType="Third Party Device", EventId="116972" Apr 6 15:40:43 192.0.2.2 : :1 Timestamp="2021-04-06 15:40:43", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:40:43 smca0 login: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost=", ReceptionTime="2021-04-06 15:40:43", SenderType="Third Party Device", EventId="116148" Apr 6 15:46:56 192.0.2.2 : :1 Timestamp="2021-04-06 15:46:56", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:46:56 smca0 login: FAILED LOGIN SESSION FROM tty1 FOR admin1 Permission denied", ReceptionTime="2021-04-06 15:46:56", SenderType="Third Party Device", EventId="116975"
Local session successful identification and authentication	Apr 6 12:35:11 192.0.2.2 : :1 Timestamp="2021-04-06 12:35:11", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 12:35:11 smca0 login: pam_unix(login:session): session opened for user test00 by LOGIN(uid=0)", ReceptionTime="2021-04-06 12:35:11", SenderType="Third Party Device", EventId="113829" Apr 6 15:39:37 192.0.2.2 : :1 Timestamp="2021-04-06 15:39:37", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:39:37 smca0 login: LOGIN ON tty1 BY test00", ReceptionTime="2021-04-06 15:39:37", SenderType="Third Party Device", EventId="115875"

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Remote session identification and authentication failures	Apr 7 16:56:56 192.0.2.2 Timestamp="2021-04-07 16:56:56", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login attempt for unknown user admin", SenderType="Management Server", EventId="3261674911353013511", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.login", Result="Fail", ObjectName="Unknown user" Apr 7 16:56:57 192.0.2.2 Timestamp="2021-04-07 16:56:57", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login attempt for unknown user admin. From 192.0.2.11.", SenderType="Management Server", SituationId="519", Situation="Management Server: Login failed", AlertSeverity="Low", EventId="1617832617690"
Remote session identification and authentication failures (continued)	Apr 7 16:58:08 192.0.2.2 Timestamp="2021-04-07 16:58:08", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="login failed for user test00. From 192.0.2.11.", SenderType="Management Server", SituationId="519", Situation="Management Server: Login failed", AlertSeverity="Low", EventId="1617832688296" Apr 7 16:58:08 192.0.2.2 Timestamp="2021-04-07 16:58:08", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login failed for user test00. ERROR: Authentication failed. The user name or password might be incorrect. Verify that the address of the server is correct and that it is running properly. ", SenderType="Management Server", EventId="3261674911353013515", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.login", Result="Fail", ObjectName="test00;Shared Domain"
Remote session identification and authentication succeeds	Apr 7 16:59:50 192.0.2.2 Timestamp="2021-04-07 16:59:50", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login succeeded for user test00 in domain Shared Domain", SenderType="Management Server", EventId="3261674911353013518", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.login", Result="Success", ObjectName="test00;Shared Domain"

FIA_X509_EXT.1	
Auditable event	Unsuccessful attempt to validate a certificate
Unsuccessful attempt to validate a certificate	Apr 7 16:10:39 192.0.2.2 Timestamp="2021-04-07 16:10:39", NodeId="192.0.2.2", CompId="Management Server", 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="Management Server", EventId="3261674911353013325", UserOriginator="System", ClientIpAddress="198.51.100.6", TypeDescription="stonegate.trusted.certificate.validation.failure", Result="Fail" Apr 8 18:07:15 192.0.2.2 Timestamp="2021-04-08 18:07:15", 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=53165] Syslog authentication failed. [/198.51.100.6:6514] Details: General SSLEngine problem Server certificate is expired", ", SenderType="Log Server", EventId="3720571525317788108", UserOriginator="System", ClientIpAddress="198.51.100.6", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"

FIA_X509_EXT.1/ITT	
Auditable event	Unsuccessful attempt to validate a certificate
Unsuccessful attempt to validate a certificate (NGFW)	Apr 9 11:35:39 192.0.2.4 Timestamp="2021-04-09 11:35:39", LogId="8290647", 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)", ReceptionTime="2021-04-09 11:35:39", SenderType="Firewall", SituationId="9000", Situation="FW_Communication-Server-Certificate-Error", EventId="6786204939375771991" Apr 9 11:35:39 192.0.2.4 Timestamp="2021-04-09 11:35:39", LogId="8290648", 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="2021-04-09 11:35:39", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6786204939375771992"

FIA_X509_EXT.1/ITT	
Unsuccessful attempt to validate a certificate (SMC)	Apr 7 10:20:48 192.0.2.2 Timestamp="2021-04-07 10:20:48", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.4 port=50794] Local = [port=3020] ERROR: Engine authentication failed. [192.0.2.4:50794] Details: Received fatal alert: unknown_ca", SenderType="Log Server", EventId="3236827228465528858", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"

FMT_MOF.1/ManualUpdate	
Auditable event	Any attempt to initiate a manual update
Any attempt to initiate a manual update	May 2 17:00:23 192.0.2.2 Timestamp="2021-05-02 17:00:23", 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 Updates and Upgrades. You are missing the following permissions: - Manage Updates and Upgrades Change your permissions or contact an administrator with the appropriate permissions to resolve this issue.", SenderType="Management Server", EventId="2649377145205329481", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.mgtserver.upgrade.import", Result="Fail", ObjectName="Engine Upgrade sg_engine_6.10.0.26021_x86-64-small.zip" Apr 30 22:10:25 192.0.2.2 Timestamp="2021-04-30 22:10:25", 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 Updates and Upgrades. You are missing the following permissions: - Manage Updates and Upgrades Change your permissions or contact an administrator with the appropriate permissions to resolve this issue.", SenderType="Management Server", EventId="2649377145205293406", UserOriginator="admin", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.mgtserver.appliance_patch.import", Result="Fail", ObjectName="SMC Appliance Patch 6.10.0T066.sap"

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

FMT_MOF.1/Functions	
Modification of the behavior of the audit functionality when Local Audit Storage Space is full	Apr 7 14:09:36 192.0.2.2 Timestamp="2021-04-07 14:09:36", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="log_spooling_policy has been modified (discard -> stop).", SenderType="Management Server", EventId="3261674911353012716", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="NGFW"
Modification of the behavior of the transmission of audit data to an external IT entity	Apr 7 14:19:54 192.0.2.2 Timestamp="2021-04-07 14:19:54", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A new log forward rule was created with All Log Data types to host Syslog (port 6514).", SenderType="Management Server", EventId="3261674911353012817", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.log.forward.new", Result="Success", ObjectName="LogServer 192.0.2.2"
Modification of the behavior of the handling of audit data	Apr 7 14:10:09 192.0.2.2 Timestamp="2021-04-07 14:10:09", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="storable_task_definition element has been created.", SenderType="Management Server", EventId="3261674911353012724", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="Delete old log and audit data" Apr 7 14:10:22 192.0.2.2 Timestamp="2021-04-07 14:10:22", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="task_schedule element has been created.", SenderType="Management Server", EventId="3261674911353012725", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="(Schedule) Delete old log and audit data"

FPT_ITT.1	
Auditable event	TLS communication between the distributed TOE components

FPT_ITT.1	
Initiation of the trusted channel (NGFW)	Apr 6 18:55:57 192.0.2.4 Timestamp="2021-04-06 18:55:57", LogId="1047456", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="TLS: Accepted connection (3 192.0.2.2)", ReceptionTime="2021-04-06 18:55:57", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6785228577338031008"
Termination of the trusted channel (NGFW)	Apr 6 18:53:15 192.0.2.4 Timestamp="2021-04-06 18:53:15", LogId="1047442", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="TLS: Connection closed (11 192.0.2.2)", ReceptionTime="2021-04-06 18:54:29", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6785227898733198226"
Failure of the trusted channel functions (NGFW)	Apr 9 10:02:18 192.0.2.4 Timestamp="2021-04-09 10:02:18", LogId="8290633", NodeId="192.0.2.4", Facility="Management", Type="Error", CompId="NGFW-FIPS node 1", InfoMsg="unsupported protocol", ReceptionTime="2021-04-09 10:02:18", SenderType="Firewall", SituationId="9005", Situation="FW_Communication-Communication-Error", EventId="6786181445904662857" Apr 9 10:02:18 192.0.2.4 Timestamp="2021-04-09 10:02:18", LogId="8290634", 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="2021-04-09 10:02:18", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6786181445904662858"

FPT_ITT.1	
Initiation of the trusted channel (SMC)	Apr 7 14:34:21 192.0.2.2 Timestamp="2021-04-07 14:34:21", 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=44420]", SenderType="Management Server", EventId="3261674911353012971", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.start", Result="Success"
Termination of the trusted channel (SMC)	Apr 7 14:32:03 192.0.2.2 Timestamp="2021-04-07 14:32:03", 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=43658]", SenderType="Management Server", EventId="3261674911353012947", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.end", Result="Success"
Failure of the trusted channel functions (SMC)	Apr 7 10:20:48 192.0.2.2 Timestamp="2021-04-07 10:20:48", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.4 port=50794] Local = [port=3020] ERROR: Engine authentication failed. [192.0.2.4:50794] Details: Received fatal alert: unknown_ca", SenderType="Log Server", EventId="3236827228465528858", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"

FPT_TUD_EXT.1	
Auditable event	Initiation of update
Verification of image (SMC)	Oct 4 13:07:07 127.0.0.1 Timestamp="2021-10-04 13:07:07", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Oct 4 13:07:07 smca AMBR_LOGGER.log : INFO : pid=5238 : Verified patch 6.10.1U001.", ReceptionTime="2021-10-04 13:07:07", SenderType="Third Party Device", EventId="10510"

FPT_TUD_EXT.1	
SMC Appliance update	Apr 1 17:07:51 192.0.2.2 : :1 Timestamp="2021-04-01 17:07:51", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 1 17:07:51 smca0 sudo: sgadmin : TTY=unknown ; PWD=/usr/local/forcepoint/smc ; USER=admin1 ; GROUP=smca_priv; COMMAND=/bin/sudo /usr/bin/ambr-load -f /usr/local/forcepoint/smc/6.10.0U001.sap", ReceptionTime="2021-04-01 17:07:51", SenderType="Third Party Device", EventId="91359" Apr 1 17:07:52 192.0.2.2 : :1 Timestamp="2021-04-01 17:07:52", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 1 17:07:52 smca0 sudo: admin1 : TTY=unknown ; PWD=/usr/local/forcepoint/smc ; USER=root ; COMMAND=/usr/bin/ambr-load -f /usr/local/forcepoint/smc/6.10.0U001.sap", ReceptionTime="2021-04-01 17:07:52", SenderType="Third Party Device", EventId="91918"
SMC Appliance update (continued)	Apr 7 16:37:43 192.0.2.2 : :1 Timestamp="2021-04-07 16:37:43", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 7 16:37:43 smca0 sudo: sgadmin : TTY=unknown ; PWD=/usr/local/forcepoint/smc ; USER=test00 ; GROUP=smca_priv ; COMMAND=/bin/sudo /usr/bin/ambr-install --no-prompt 6.10.0U001", ReceptionTime="2021-04-07 16:37:43", SenderType="Third Party Device", EventId="20597" Apr 7 16:37:43 192.0.2.2 : :1 Timestamp="2021-04-07 16:37:43", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 7 16:37:43 smca0 sudo: test00 : TTY=unknown ; PWD=/usr/local/forcepoint/smc ; USER=root ; COMMAND=/usr/bin/ambr-install --no-prompt 6.10.0U001", ReceptionTime="2021-04-07 16:37:43", SenderType="Third Party Device", EventId="20605"

FPT_TUD_EXT.1	
Successful SMC update	Oct 4 13:07:26 127.0.0.1 Timestamp="2021-10-04 13:07:26", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Oct 4 13:07:26 smca AMBR_LOGGER.log : INFO : pid=5238 : Installed patch 6.10.1U001.", ReceptionTime="2021-10-04 13:07:26", SenderType="Third Party Device", EventId="10539" Oct 4 13:09:47 127.0.0.1 Timestamp="2021-10-04 13:09:47", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Oct 4 13:09:47 smca AMBR_LOGGER.log : INFO : pid=5238 : Successfully installed patch(es): 6.10.1U001.", ReceptionTime="2021-10-04 13:09:47", SenderType="Third Party Device", EventId="10610"
Failed SMC Appliance update	Apr 7 16:39:37 192.0.2.2 : :1 Timestamp="2021-04-07 16:39:37", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 7 16:39:37 smca0 AMBR_LOGGER.log : ERROR : pid=41642 : No valid signer certificates for '/var/tmp/tmptor7ki45/6.10.0T066.sap'#012Traceback (most recent call last):#012 File 'build/lib/ambr/client/load/application.py' line 118 in _load_local#012 File 'build/lib/ambr/client/load/application.py' line 214 in _fetch_metadata#012 File 'build/lib/ambr/common/crypto.py' line 247 in verify_package#012ValueError: No valid signer certificates for '/var/tmp/ tmptor7ki45/6.10.0T066.sap'", ReceptionTime="2021-04-07 16:39:37", SenderType="Third Party Device", EventId="20642" Apr 7 16:39:37 192.0.2.2 : :1 Timestamp="2021-04-07 16:39:37", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 7 16:39:37 smca0 AMBR_LOGGER.log : ERROR : pid=41642 : Failed to load: /usr/local/forcepoint/smc/6.10.0T066.sap", ReceptionTime="2021-04-07 16:39:37", SenderType="Third Party Device", EventId="20643" Apr 7 16:39:37 192.0.2.2 Timestamp="2021-04-07 16:39:37", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="ERROR: Unable to get issuer certificate for 'C=US ST=TX L=Austin O=Forcepoint OU=NGFW CN=NGFW Test Updates'ERROR: Unable to load /usr/local/ forcepoint/smc/6.10.0T066.sap to /var/ambr/downloaded.ERROR: No valid signer certificates for '/var/tmp/tmptor7ki45/6.10.0T066.sap'ERROR: Failed to load: / usr/local/forcepoint/smc/6.10.0T066.sap", SenderType="Management Server", EventId="3261674911353013442", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.mgtserver.appliance_patch.import", Result="Fail"

FPT_TUD_EXT.1	
Verification of image (NGFW Engine)	Oct 4 14:25:14 192.0.2.4 Timestamp="2021-10-04 14:25:14", LogId="207", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW node 1", InfoMsg="Engine upgrade: Engine image signature verified", ReceptionTime="2021-10-04 14:25:15", SenderType="Firewall", SituationId="40015", Situation="System_Engine_Upgrade-Succeeded", EventId="6850752658534301903"
Initiation of NGFW Engine update	Apr 7 14:29:44 192.0.2.2 Timestamp="2021-04-07 14:29:44", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Image sg_engine_6.10.0.26018_x86-64-small.zip", SenderType="Management Server", EventId="3261674911353012923", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.engine.upgrade.start", Result="Success", ObjectName="NGFW node 1"
Result of the NGFW Engine update attempt	Apr 7 14:34:20 192.0.2.2 Timestamp="2021-04-07 14:34:20", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Image StoneGate firewall(x86-64-small) version 6.10 #26018", SenderType="Management Server", EventId="3261674911353012970", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.engine.upgrade.end", Result="Success", ObjectName="NGFW node 1"
Failed NGFW Engine update	Jan 20 11:21:37 192.0.2.2 Timestamp="2023-01-20 11:21:37", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Signature verification failed for the Update Package or Engine Upgrade Trust anchor for certification path not found.", SenderType="Management Server", EventId="5618505504562086431", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.mgtserver.upgrade.import", Result="Fail", ObjectName="Engine Upgrade sg_engine_6.11.0.27009.invalid.1_x86-64-small.zip"

FTA_SSL.3	
Auditable event	The termination of a remote session by session locking mechanism

FTA_SSL.3	
Termination of a remote session by session locking mechanism	Apr 7 16:16:38 192.0.2.2 Timestamp="2021-04-07 16:16:38", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Management Client window closed due to idle timeout.", SenderType="Management Server", EventId="3261674911353013344", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.session.terminated", Result="Success", ObjectName="admin1"

FTA_SSL.4	
Auditable event	The termination of an interactive session
Termination of local administrative session	Apr 6 15:39:24 192.0.2.2 : :1 Timestamp="2021-04-06 15:39:24", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:39:24 smca0 login: pam_unix(login:session): session closed for user test00", ReceptionTime="2021-04-06 15:39:24", SenderType="Third Party Device", EventId="115072"
Termination of remote administrative session	Apr 7 15:48:35 192.0.2.2 Timestamp="2021-04-07 15:48:35", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Logout succeeded for user admin2.", SenderType="Management Server", EventId="3261674911353013224", UserOriginator="System", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.admin.logout", Result="Success", ObjectName="admin2"

FTA_SSL_EXT.1	
Auditable event	Local session termination

FTA_SSL_EXT.1	
Local session termination	Apr 6 15:40:37 192.0.2.2 : :1 Timestamp="2021-04-06 15:40:37", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:40:37 smca0 audisp-syslog: type=PATH msg=audit(1617741637.003:22873): item=1 name='/var/run/console/ console.lock' inode=1306884 dev=00:17 mode=0100600 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:pam_var_console_t:s0 nametype=DELETE cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0 OUID='root' OGID='root'", ReceptionTime="2021-04-06 15:40:37", SenderType="Third Party Device", EventId="115907" Apr 6 15:40:37 192.0.2.2 : :1 Timestamp="2021-04-06 15:40:37", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:40:37 smca0 login: pam_unix(login:session): session closed for user test00", ReceptionTime="2021-04-06 15:40:37", SenderType="Third Party Device", EventId="115910" Apr 6 15:40:37 192.0.2.2 : :1 Timestamp="2021-04-06 15:40:37", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 6 15:40:37 smca0 audisp-syslog: type=USER_END msg=audit(1617741637.010:22874): pid=531330 uid=0 auid=1000 ses=142 subj=system_u:system_r:local_login_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_selinux pam_loginuid pam_selinux pam_namespace pam_keyinit pam_keyinit pam_limits pam_systemd pam_unix pam_umask pam_lastlog acct='test00' exe='/usr/bin/login' hostname=smca0 addr=? terminal=tty1 res=success' UID='root' AUID='test00'", ReceptionTime="2021-04-06 15:40:37", SenderType="Third Party Device", EventId="115911"

FTP_ITC.1	
Auditable event	Trusted channel functions
Initiation of the trusted channel	Apr 7 14:34:21 192.0.2.2 Timestamp="2021-04-07 14:34:21", 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=44420]", SenderType="Management Server", EventId="3261674911353012971", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.start", Result="Success"

FTP_ITC.1	
Termination of the trusted channel	Apr 7 14:32:03 192.0.2.2 Timestamp="2021-04-07 14:32:03", 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=43658]", SenderType="Management Server", EventId="3261674911353012947", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.end", Result="Success"
Auditable event	Failure of the trusted channel functions
TLS failure	Apr 7 16:05:39 192.0.2.2 Timestamp="2021-04-07 16:05:39", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.10 port=6514] Local = [port=54854] Syslog authentication failed. [192.0.2.10:6514] Details: Received fatal alert: handshake_failure", SenderType="Management Server", EventId="3261674911353013303", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"
Connection failure	Apr 7 16:07:38 192.0.2.2 Timestamp="2021-04-07 16:07:38", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Connection failed : Peer = [host=192.0.2.10 port=6514] Local = [port=35430] Client requested protocol Connection refused. [192.0.2.10:6514]", SenderType="Management Server", EventId="3261674911353013312", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.connection.failure", Result="Fail"

FTP_TRP.1/Admin	
Auditable event	Trusted path functions
Initiation of the trusted path	Apr 7 11:06:06 192.0.2.2 Timestamp="2021-04-07 11:06:06", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.10 port=514] Local = [host=192.0.2.2 port=58104]", SenderType="Management Server", EventId="3248529000007467015", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.start", Result="Success"

FTP_TRP.1/Admin	
Termination of the trusted path	Apr 7 14:20:06 192.0.2.2 Timestamp="2021-04-07 14:20:06", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.10 port=514] Local = [host=192.0.2.2 port=39768]", SenderType="Management Server", EventId="3291990216457322597", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.end", Result="Success"
Failure of the trusted path functions	Apr 7 15:50:23 192.0.2.2 Timestamp="2021-04-07 15:50:23", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.10 port=41562] Local = [port=8905] ERROR: Client requested protocol TLSv1.1 is not enabled or supported in server context", SenderType="Management Server", EventId="3261674911353013242", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"

FTP_TRP.1/Join	
Auditable event	Trusted path functions
SMC registration (Initiation)	Oct 4 14:11:46 192.0.2.2 Timestamp="2021-10-04 14:11:46", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=54728] Local = [host=192.0.2.2 port=3021]", SenderType="Management Server", EventId="5397881555781681360", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.start", Result="Success"
SMC registration (Termination)	Oct 4 14:11:46 192.0.2.2 Timestamp="2021-10-04 14:11:46", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=54728] Local = [port=3021]", SenderType="Management Server", EventId="5397881555781681362", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.end", Result="Success"

FTP_TRP.1/Join	
SMC registration (Failure)	Oct 4 14:06:50 192.0.2.2 Timestamp="2021-10-04 14:06:50",NodeId="192.0.2.2", CompId="Management Server", InfoMsg="The one-time password is invalid.", SenderType="Management Server", EventId="5397881555781681343", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.engine.initial.contact", Result="Fail" Oct 4 14:06:50 192.0.2.2 Timestamp="2021-10-04 14:06:50", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=54720] Local = [port=3021]", SenderType="Management Server", EventId="5397881555781681344", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.end", Result="Success"
NGFW Engine registration (Initiation)	Oct 5 17:47:43 192.0.2.4 Timestamp="2022-10-05 17:47:43", LogId="781", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="0", InfoMsg="TLS: Connected connection (N/A 192.0.2.2)", ReceptionTime="2022-10-05 17:48:58", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6983437568540934925"
NGFW Engine registration (Termination)	Oct 5 17:47:46 192.0.2.4 Timestamp="2022-10-05 17:47:46", LogId="785", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="0", InfoMsg="TLS: Connection disconnect (N/A 192.0.2.2)", ReceptionTime="2022-10-05 17:48:58", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6983437581425836817"

FTP_TRP.1/Join	
NGFW Engine registration (Failure)	Oct 5 17:45:07 192.0.2.4 Timestamp="2022-10-05 17:45:07", LogId="675", NodeId="192.0.2.4", Facility="Management", Type="Error", CompId="0", InfoMsg="sslv3 alert handshake failure", ReceptionTime="2022-10-05 17:48:58", SenderType="Firewall", SituationId="9005", Situation="FW_Communication-Communication-Error", EventId="6983436915705905827" Oct 5 17:45:07 192.0.2.4 Timestamp="2022-10-05 17:45:07", LogId="676", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="0", InfoMsg="TLS: Couldn't connect TLS connection: -3 (N/A 192.0.2.2)", ReceptionTime="2022-10-05 17:48:58", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="6983436915705905828"

FCO_CPC_EXT.1	
Auditable event	Enabling and disabling communication between the NGFW Engine and SMC.
Enabling from the NGFW Engine	Apr 9 12:05:29 192.0.2.4 Timestamp="2021-04-09 12:05:29", LogId="8290670", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="Connection to Management Server (192.0.2.2) enabled", ReceptionTime="2021-04-09 12:05:29", SenderType="Firewall", EventId="6786212446978605422" Apr 9 12:09:41 192.0.2.4 Timestamp="2021-04-09 12:09:41", LogId="8290770", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="Connection to Log Server (192.0.2.2) enabled", ReceptionTime="2021-04-09 12:09:41", SenderType="Firewall", EventId="6786213503540560338"

FCO_CPC_EXT.1	
Disabling from the NGFW Engine	Apr 9 12:21:13 192.0.2.4 Timestamp="2021-04-09 12:21:13", LogId="8290919", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="Engine factory reset initiated from SMC", ReceptionTime="2021-04-09 12:21:13", SenderType="Firewall", SituationId="500", Situation="FW_Notice", EventId="6786216402643485287" Apr 9 12:21:13 192.0.2.4 Timestamp="2021-04-09 12:21:13", LogId="8290920", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="Connection to Management Server (192.0.2.2) and Log Server disabled", ReceptionTime="2021-04-09 12:21:13", SenderType="Firewall", SituationId="500", Situation="FW_Notice", EventId="6786216402643485288"
Enabling from the SMC	Apr 7 13:48:35 192.0.2.2 Timestamp="2021-04-07 13:48:35", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Initial configuration generated for Firewall engine", SenderType="Management Server", EventId="3261674911353012468", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.engine.initial.generate", Result="Success", ObjectName="NGFW" Apr 7 13:50:33 192.0.2.2 Timestamp="2021-04-07 13:50:33", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Initial contact from Firewall Node", SenderType="Management Server", EventId="3261674911353012486", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.engine.initial.contact", Result="Success", ObjectName="NGFW node 1"

FCO_CPC_EXT.1	
Disabling from the SMC	Apr 7 17:44:44 192.0.2.2 Timestamp="2021-04-07 17:44:44", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353013706", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.firewall.Reset Engine to Factory Settings", Result="Success", ObjectName="NGFW node 1" Apr 7 17:45:05 192.0.2.2 Timestamp="2021-04-07 17:45:05", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353013709", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.object.delete", Result="Success", ObjectName="NGFW" Apr 7 17:45:05 192.0.2.2 Timestamp="2021-04-07 17:45:05", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="3261674911353013711", UserOriginator="test00", ClientIpAddress="192.0.2.11", TypeDescription="stonegate.license.unbind", Result="Success", ObjectName="NGFW node 1"

FCS_IPSEC_EXT.1 IPsec Protocol	
Auditable event	
Decisions to DISCARD network packets processed by the TOE	**DISCARD** Apr 4 10:21:05 192.0.2.4 Timestamp="2023-04-04 10:21:05", LogId="513964", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="Connection discarded", Action="Discard", Protocol="6", Src="203.0.113.100", Dst="198.51.100.100", Sport="53098", Dport="80", RuleId="2097171.0", Srcif="2", CompId="NGFW node 1", ReceptionTime="2023-04-04 10:21:06", SenderType="Firewall", SituationId="70019", Situation="Connection_Discarded",EventId="7048917377215365298", Service="HTTP"

FCS_IPSEC_EXT.1 IPsec Protocol	
Decisions to BYPASS network packets processed by the TOE	**BYPASS** Apr 4 10:35:51 192.0.2.4 Timestamp="2023-04-04 10:35:51", LogId="514333", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="New connection", Action="Allow",Protocol="6", Src="198.51.100.100", Dst="203.0.113.100", Sport="60290", Dport="80", RuleId="2097195.1", Srcif="1", CompId="NGFW node 1", ReceptionTime="2023-04-04 10:35:51", SenderType="Firewall", SituationId="70018", Situation="Connection_Allowed", EventId="7048921092362076452",Service="HTTP"
Decisions to PROTECT network packets processed by the TOE	**PROTECT** Apr 4 11:42:56 192.0.2.4 Timestamp="2023-04-04 11:42:56", LogId="515622", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="New connection through VPN", Action="Allow", Protocol="6",Src="10.0.51.100", Dst="198.51.100.100", Sport="50686", Dport="80", RuleId="2097192.0", CompId="NGFW node 1", ReceptionTime="2023-04-04 11:42:56", SenderType="Firewall", SituationId="71012", Situation="FW_New-IPsec-VPN-Connection", EventId="7048937975878517657", Service="HTTP"

FCS_IPSEC_EXT.1 IPsec Protocol	
IPsec SAs	**Failure to establish an IPsec SA** Sep 12 18:21:05 192.0.2.4 Timestamp="2022-09-12 18:21:05", LogId="96365", NodeId="192.0.2.4", Facility="IPsec VPN", Type="Error", Src="203.0.113.100", Dst="203.0.113.4", Sport="500", Dport="500", CompId="NGFW node 1", InfoMsg="IKEv2 SA error: No proposal chosen: Remote Traffic Selector mismatch (80) tunnel ID 1073709063", ReceptionTime="2022-09-12 18:21:05", SenderType="Firewall", SituationId="12166", Situation="IKE-No-Proposal-Chosen", EventId="6975111048588261485" Sep 12 18:21:05 192.0.2.4 Timestamp="2022-09-12 18:21:05", LogId="96367", NodeId="192.0.2.4", Facility="IPsec VPN", Type="Error", Src="203.0.113.100", Dst="203.0.113.4", Sport="500", Dport="500", CompId="NGFW node 1", InfoMsg="IPsec SA error: No proposal chosen", ReceptionTime="2022-09-12 18:21:05", SenderType="Firewall", SituationId="12166", Situation="IKE-No-Proposal-Chosen", EventId="6975111048588261487"

FCS_IPSEC_EXT.1 IPsec Protocol	
	IPsec SA establishment 192.0.2.4", Facility="IPsec VPN", Type="Notification", Src="203.0.113.100", Dst`="203.0.113.4", Sport="500", Dport="500", CompId="NGFW node 1", InfoMsg="IKEv2 SA responder done Local ngfw.local (fqdn) Remote vpngw.local (fqdn) Local auth method: DSA Elliptic Curve ECP signature Remote auth method: DSA Elliptic Curve ECP signature Local signature algorithm: ecdsa-with-SHA384 Remote signature algorithm: ecdsa-with-SHA384 lifetime 86400 secs", ReceptionTime="2022-09-09 20:20:05", SenderType="Firewall", SituationId="12102", Situation="IKE-SA-Responder-Done", EventId="6974053829503448321" Sep 9 20:20:05 192.0.2.4 Timestamp="2022-09-09 20:20:05", LogId="95490", NodeId="192.0.2.4", Facility="IPsec VPN", Type="Notification", Src="10.0.51.0", Dst="198.51.100.0",CompId="NGFW node 1", InfoMsg="IPsec SA responder done. Encryption:aes256-gcm mac:none. Negotiation took 3 msecs.", ReceptionTime="2022-09-09 20:20:05", SenderType="Firewall", SituationId="12107", Situation="IPsec-SA-Responder-Done", EventId="6974053829503448322"

FCS_IPSEC_EXT.1 IPsec Protocol	
	IPsec SA termination Sep 9 20:21:39 192.0.2.4 Timestamp="2022-09-09 20:21:39", LogId="95495", NodeId="192.0.2.4", Facility="IPsec VPN", Type="Notification", Src="203.0.113.100", Dst="203.0.113.4", Sport="500", Dport="500", CompId="NGFW node 1", InfoMsg="IKE SA deleted", ReceptionTime="2022-09-09 20:21:39", SenderType="Firewall", SituationId="12116", Situation="IKE-SA-Deleted", EventId="6974054224640439559" Sep 9 20:21:29 192.0.2.4 Timestamp="2022-09-09 20:21:29", LogId="95494", NodeId="192.0.2.4", Facility="IPsec VPN", Type="Notification", Src="203.0.113.100", Dst="203.0.113.4", Sport="500", Dport="500", CompId="NGFW node 1", InfoMsg="IPsec SA deleted", ReceptionTime="2022-09-09 20:21:29", SenderType="Firewall", SituationId="12117", Situation="IPsec-SA-Deleted", EventId="6974054181690766598"

FIA_X509_EXT.1/Rev X.509 Certificate Validation (VPN)	
Auditable event	**Unsuccessful attempt to validate a certificate**

FIA_X509_EXT.1/Rev X.509 Certificate Validation (VPN)	
Unsuccessful attempt to validate a peer certificate	Sep 12 18:55:21 192.0.2.4 Timestamp="2022-09-12 18:55:21", LogId="96716", NodeId="192.0.2.4", Facility="IPsec VPN", Type="Error", Src="203.0.113.100", Dst="203.0.113.4", Sport="500", Dport="500", CompId="NGFW node 1", InfoMsg="Validating certificate with subject='C=US O=Forcepoint OU=NGFW CN=vpngw.local' failed. Reason: (did not find trusted CA CRL was not found path was not verified)", ReceptionTime="2022-09-12 18:55:21", SenderType="Firewall", SituationId="12168", Situation="IKE-Authentication-Failed", EventId="6975119668587624908" Sep 12 18:55:21 192.0.2.4 Timestamp="2022-09-12 18:55:21", LogId="96717", NodeId="192.0.2.4", Facility="IPsec VPN", Type="Error", Src="203.0.113.100", Dst="203.0.113.4", Sport="500", Dport="500", CompId="NGFW node 1", InfoMsg="Certificate lookup errors: did not find trusted CA CRL was not found path was not verified", ReceptionTime="2022-09-12 18:55:21", SenderType="Firewall", EventId="6975119668587624909" Sep 12 18:55:21 192.0.2.4 Timestamp="2022-09-12 18:55:21", LogId="96718", NodeId="192.0.2.4", Facility="IPsec VPN", Type="Error", Src="203.0.113.100", Dst="203.0.113.4", Sport="500", Dport="500", CompId="NGFW node 1", InfoMsg="IKEv2 SA error: Authentication failed", ReceptionTime="2022-09-12 18:55:21", SenderType="Firewall", SituationId="12168", Situation="IKE-Authentication-Failed", EventId="6975119668587624910"

FIA_X509_EXT.1/Rev X.509 Certificate Validation (VPN)	
Any addition, replacement or removal of trust anchors in the TOE's trust store	**Import of a trusted certificate authority** Sep 6 12:18:36 192.0.2.2 Timestamp="2022-09-06 12:18:36", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="certificate_authority element has been created.", SenderType="Management Server", EventId="1263692714080207756", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="VPN Root CA" Sep 6 12:18:37 192.0.2.2 Timestamp="2022-09-06 12:18:37", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A local certificate key was imported into a VPN Certificate Authority.", SenderType="Management Server", EventId="1300998963222020099", UserOriginator="admin", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.certificate.import", Result="Success", ObjectName="VPN Root CA"
	Configuration of trusted certificate authorities Oct 04 12:45:49 192.0.2.2 Timestamp="2022-10-04 12:45:49", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="certificate_authority_ref has been removed: <certificate_authority_ref ref='VPN GW Root CA 3 (RSA)'/>.", SenderType="Management Server", EventId="2440705089682277420", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Forcepoint VPN Profile" Oct 04 12:46:11 192.0.2.2 Timestamp="2022-10-04 12:46:11", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="certificate_authority_ref has been modified on its attribute: ref (VPN GW Root CA 1 (RSA) -> VPN GW Root CA 2 (RSA)).", SenderType="Management Server", EventId="2440705089682277423", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Forcepoint VPN Profile"

FIA_X509_EXT.1/Rev X.509 Certificate Validation (VPN)	
	Removal (deletion) of a trusted certificate authority Oct 04 12:52:07 192.0.2.2 Timestamp="2022-10-04 12:52:07", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="2440705089682277450", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.cryptographic_key.deleted", Result="Success", ObjectName="VPN GW Root CA 3 (RSA)" Oct 04 12:52:07 192.0.2.2 Timestamp="2022-10-04 12:52:07", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Certificate with subject name CN=VPN GW Root CA 2 O=Forcepoint C=US.", SenderType="Management Server", EventId="2440705089682277451", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.certificate.delete", Result="Success", ObjectName="Certificate <CN=VPN GW Root CA 2 O=Forcepoint C=US> (2043-04-06)" Oct 04 12:52:07 192.0.2.2 Timestamp="2022-10-04 12:52:07", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="2440705089682277449", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.delete", Result="Success", ObjectName="VPN GW Root CA 3 (RSA)"

FMT SMF.1/VPN FAU_GEN.1.1 c) All administrative actions (VPN)	
Auditable event	**Generating / import of, changing, or deleting of cryptographic keys**
Generating / import of, changing, or deleting of cryptographic keys	**Creation of a VPN private key** Sep 6 16:11:07 192.0.2.4 Timestamp="2022-09-06 16:11:07", LogId="84557", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="NGFW node 1", InfoMsg="Private key /data/config/ipsec/priv/ request20220906041106014190833497O.prv has been created", ReceptionTime="2022-09-06 16:11:07", SenderType="Firewall", SituationId="40010", Situation="System_Engine-Cryptkeys-Created", EventId="6972904015218690637"

<table>
<tr><th colspan="2">FMT SMF.1/VPN FAU_GEN.1.1 c) All administrative actions (VPN)</th></tr>
<tr><td rowspan="2"></td><td>Certificate signing request
<pre>Sep 6 16:11:07 192.0.2.2 Timestamp="2022-09-06 16:11:07",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="Certificate Request requested to Firewall.",
SenderType="Management Server",
EventId="1263692714080208936",
UserOriginator="System",
ClientIpAddress="192.0.2.2",
TypeDescription="stonegate.vpn.certificate.request",
Result="Success",
ObjectName="NGFW;Certificate Request <C=US O=Forcepoint OU=NGFW CN=ngfw.local>
 ECDSA / SHA384"</pre><pre>Sep 6 16:11:07 192.0.2.2 Timestamp="2022-09-06 16:11:07",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="certificate_request element has been created.",
SenderType="Management Server",
EventId="1263692714080208935",
UserOriginator="System",
ClientIpAddress="192.0.2.2",
TypeDescription="stonegate.object.insert",
Result="Success",
ObjectName="Certificate Request <C=US O=Forcepoint OU=NGFW CN=ngfw.local>
 ECDSA / SHA384"</pre></td></tr>
<tr><td>Import of a signed certificate
<pre>Sep 6 16:46:11 192.0.2.2 Timestamp="2022-09-06 16:46:11",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="certificate element has been created.",
SenderType="Management Server",
EventId="1263692714080208968",
UserOriginator="admin",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.insert",
Result="Success",
ObjectName="Certificate <C=US O=Forcepoint OU=NGFW CN=ngfw.local> ECDSA /
 SHA384 (2023-09-06)"</pre></td></tr>
<tr><td>Configuration of remote VPN client session timeout</td><td><pre>Sep 27 09:18:26 192.0.2.2 Timestamp="2022-09-27 09:18:26",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="web_authentication has been modified on its attribute:
 authentication_idle_timeout (1800 -> 3600).",
SenderType="Management Server",
EventId="8672153962696158209",
UserOriginator="root",
ClientIpAddress="192.0.2.85",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="NGFW-FIPS"</pre></td></tr>
</table>

FMT SMF.1/VPN FAU_GEN.1.1 c) All administrative actions (VPN)	
Configuration of the cryptographic functionality	**Configuration of IPSec functionality** Sep 27 09:11:20 192.0.2.2 Timestamp="2022-09-27 09:11:20", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="capabilities has been modified on its attribute: sha2_for_ipsec (false -> true).", SenderType="Management Server", EventId="8672153962696158169", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Forcepoint VPN Profile" Sep 27 09:11:20 192.0.2.2 Timestamp="2022-09-27 09:11:20", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="capabilities has been modified on its attribute: aes256_for_ipsec (false -> true).", SenderType="Management Server", EventId="8672153962696158171", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Forcepoint VPN Profile" Sep 27 09:11:20 192.0.2.2 Timestamp="2022-09-27 09:11:20", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="capabilities has been modified on its attribute: sha1_for_ipsec (true -> false).", SenderType="Management Server", EventId="8672153962696158170", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Forcepoint VPN Profile" Sep 27 09:13:17 192.0.2.2 Timestamp="2022-09-27 09:13:17", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="capabilities has been modified on its attribute: sha2_ipsec_hash_length (256 -> 512).", SenderType="Management Server", EventId="8672153962696158182", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Forcepoint VPN Profile"

FMT SMF.1/VPN FAU_GEN.1.1 c) All administrative actions (VPN)	
Configuration of the lifetime for IKEv2 SAs	**Configuration of IKEv2 SA lifetimes** `Sep 27 09:09:00 192.0.2.2 Timestamp="2022-09-27 09:09:00", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="sa_life_time has been modified (86400 -> 43200).", SenderType="Management Server", EventId="8672153962696158149", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Forcepoint VPN Profile"`
	Configuring IKEv2 Child SA lifetimes `Sep 27 09:09:00 192.0.2.2 Timestamp="2022-09-27 09:09:00", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="sa_life_time has been modified (86400 -> 43200).", SenderType="Management Server", EventId="8672153962696158149", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Forcepoint VPN Profile"`
	Configuring IKEv2 Child SA lifetimes `Sep 27 09:09:00 192.0.2.2 Timestamp="2022-09-27 09:09:00", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="tunnel_life_time_seconds has been modified (28800 -> 21600).", SenderType="Management Server", EventId="8672153962696158148", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Forcepoint VPN Profile"` `Sep 27 09:09:00 192.0.2.2 Timestamp="2022-09-27 09:09:00", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="tunnel_life_time_kbytes has been modified (0 -> 1024000).", SenderType="Management Server", EventId="8672153962696158150", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Forcepoint VPN Profile"`

FPF_RUL_EXT.1 Packet Filtering Rules	
Auditable event	**Application of rules configured with the log operation**

<table>
<tr><th colspan="2">FPF_RUL_EXT.1 Packet Filtering Rules</th></tr>
<tr><td rowspan="2">Application of rules configured with the 'log' operation (VPN)</td><td>Drop traffic
<pre>Apr 4 10:21:05 192.0.2.4 Timestamp="2023-04-04 10:21:05",
LogId="513964",
NodeId="192.0.2.4",
Facility="Packet Filtering",
Type="Notification",
Event="Connection discarded",
Action="Discard",
Protocol="6",
Src="203.0.113.100",
Dst="198.51.100.100",
Sport="53098",
Dport="80",
RuleId="2097171.0",
Srcif="2",
CompId="NGFW node 1",
ReceptionTime="2023-04-04 10:21:06",
SenderType="Firewall",
SituationId="70019",
Situation="Connection_Discarded",
EventId="7048917377215365298",
Service="HTTP"</pre></td></tr>
<tr><td>Permit traffic (BYPASS)
<pre>Apr 4 10:35:51 192.0.2.4 Timestamp="2023-04-04 10:35:51",
LogId="514333",
NodeId="192.0.2.4",
Facility="Packet Filtering",
Type="Notification",
Event="New connection",
Action="Allow",
Protocol="6",
Src="198.51.100.100",
Dst="203.0.113.100",
Sport="60290",
Dport="80",
RuleId="2097195.1",
Srcif="1",
CompId="NGFW node 1",
ReceptionTime="2023-04-04 10:35:51",
SenderType="Firewall",
SituationId="70018",
Situation="Connection_Allowed",
EventId="7048921092362076452",
Service="HTTP"</pre></td></tr>
</table>

FPF_RUL_EXT.1 Packet Filtering Rules	
	Permit traffic (PROTECT) Apr 4 11:42:56 192.0.2.4 Timestamp="2023-04-04 11:42:56", LogId="515622", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="New connection through VPN", Action="Allow", Protocol="6", Src="10.0.51.100", Dst="198.51.100.100", Sport="50686", Dport="80", RuleId="2097192.0", CompId="NGFW node 1", ReceptionTime="2023-04-04 11:42:56", SenderType="Firewall", SituationId="71012", Situation="FW_New-IPsec-VPN-Connection", EventId="7048937975878517657", Service="HTTP"

FTP_ITC.1/VPN Inter-TSF Trusted Channel (VPN Communications)	
Auditable event	**Trusted channel functions**
Initiation of the trusted channel	192.0.2.4", Facility="IPsec VPN", Type="Notification", Src="203.0.113.100", Dst="203.0.113.4", Sport="500", Dport="500", CompId="NGFW node 1", InfoMsg="IKEv2 SA responder done Local ngfw.local (fqdn) Remote vpngw.local (fqdn) Local auth method: DSA Elliptic Curve ECP signature Remote auth method: DSA Elliptic Curve ECP signature Local signature algorithm: ecdsa-with-SHA384 Remote signature algorithm: ecdsa-with-SHA384 lifetime 86400 secs", ReceptionTime="2022-09-09 20:20:05", SenderType="Firewall", SituationId="12102", Situation="IKE-SA-Responder-Done", EventId="6974053829503448321"
Termination of the trusted channel	Sep 9 20:21:39 192.0.2.4 Timestamp="2022-09-09 20:21:39", LogId="95495", NodeId="192.0.2.4", Facility="IPsec VPN", Type="Notification", Src="203.0.113.100", Dst="203.0.113.4", Sport="500", Dport="500", CompId="NGFW node 1", InfoMsg="IKE SA deleted", ReceptionTime="2022-09-09 20:21:39", SenderType="Firewall", SituationId="12116", Situation="IKE-SA-Deleted", EventId="6974054224640439559"

FTP_ITC.1/VPN Inter-TSF Trusted Channel (VPN Communications)	

Failure of the trusted channel functions	<pre>Sep 9 20:10:28 192.0.2.4 Timestamp="2022-09-09 20:10:28",
	LogId="95374",
	NodeId="192.0.2.4",
	Facility="IPsec VPN",
	Type="Error",
	Src="203.0.113.100",
	Dst="203.0.113.4",
	Sport="500",
	Dport="500",
	CompId="NGFW node 1",
	InfoMsg="No rule found for selectors ipv4(198.51.100.0-198.51.100.255) <->
	ipv4(10.0.51.0-10.0.51.255) and for IKE peers 203.0.113.4 and 203.0.113.100
	and IKE IDs local ngfw.local (fqdn) and remote vpngw.local (fqdn): No IPsec
	rules configured",
	ReceptionTime="2022-09-09 20:10:28",
	SenderType="Firewall",
	EventId="6974051411436860558"</pre>
	<pre>Sep 9 20:10:28 192.0.2.4 Timestamp="2022-09-09 20:10:28",
	LogId="95376",
	NodeId="192.0.2.4",
	Facility="IPsec VPN",
	Type="Error",
	Src="203.0.113.100",
	Dst="203.0.113.4",
	Sport="500",
	Dport="500",
	CompId="NGFW node 1",
	InfoMsg="IKEv2 SA error: No proposal chosen: No IPsec rules configured (7fff)
	tunnel ID 1073709062",
	ReceptionTime="2022-09-09 20:10:28",
	SenderType="Firewall",
	SituationId="12166",
	Situation="IKE-No-Proposal-Chosen",
	EventId="6974051411436860560"</pre>

FTA_TSE.1.1 TOE Session Establishment	
Auditable event	

<table>
<tr><th colspan="2">FTA_TSE.1.1 TOE Session Establishment</th></tr>
<tr><td>Configuration of attributes used to deny establishment of remote VPN client session (location, time, day)</td><td>Configuration of attributes used to deny establishment of remote VPN client session (time, day)
<pre>Sep 27 10:39:36 192.0.2.2 Timestamp="2022-09-27 10:39:36",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="rule_entry has been added:
<rule_entry is_disabled='false' rank='1.875' rule_tag_major_id='239' tag='239.0'>
<match_part><match_sources>
<match_source_ref type='network_element' value='Forcepoint_site2_net'/>
</match_sources>
<match_destinations>
<match_destination_ref type='network_element' value='$$ Local Cluster(NDI
 addresses only)'/>
</match_destinations>
<match_services>
<match_service_ref type='service' value='ISAKMP (UDP)'/>
<match_service_ref type='service' value='NAT-T (Destination)'/>
</match_services>
<rule_validity_times>
<rule_validity_time_ref type='rule_validity_time' value='After office hours'/>
<rule_validity_time_ref type='rule_validity_time' value='Before office hours'/>
</rule_validity_times></match_part><option>
<log_policy log_compression='off' log_level='stored' mss_enforce='false'/></
option>
</rule_entry>.",
SenderType="Management Server",
EventId="8672153962696158430",
UserOriginator="root",
ClientIpAddress="192.0.2.85",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="Firewall cPP Template"</pre></td></tr>
<tr><td>Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)</td><td><pre>Sep 27 10:43:17 192.0.2.2 Timestamp="2022-09-27 10:43:17",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="rule_validity_time element has been created.",
SenderType="Management Server",
EventId="8672153962696158435",
UserOriginator="root",
ClientIpAddress="192.0.2.85",
TypeDescription="stonegate.object.insert",
Result="Success",
ObjectName="Weekends"</pre></td></tr>
<tr><td>Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)</td><td><pre>Sep 27 10:43:29 192.0.2.2 Timestamp="2022-09-27 10:43:29",
NodeId="192.0.2.2",
CompId="Management Server",
SenderType="Management Server",
EventId="8672153962696158438",
UserOriginator="root",
ClientIpAddress="192.0.2.85",
TypeDescription="stonegate.object.update",
Result="Success",
ObjectName="After office hours"</pre></td></tr>
</table>

FTA_TSE.1.1 TOE Session Establishment	
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	Sep 27 10:43:29 192.0.2.2 Timestamp="2022-09-27 10:43:29", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="week_day has been modified (mo tu we th fr sa su -> mo tu we th fr).", SenderType="Management Server", EventId="8672153962696158437", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="After office hours"
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	Sep 27 10:43:36 192.0.2.2 Timestamp="2022-09-27 10:43:36", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="rule_time_repeat_end has been modified (07:00 -> 06:00).", SenderType="Management Server", EventId="8672153962696158439", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Before office hours"
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	Sep 27 10:43:36 192.0.2.2 Timestamp="2022-09-27 10:43:36", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8672153962696158440", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update", Result="Success", ObjectName="Before office hours"
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	Sep 27 10:43:59 192.0.2.2 Timestamp="2022-09-27 10:43:59", NodeId="192.0.2.2", RuleId="239.1", CompId="Management Server", InfoMsg="IPv4 Access Rule @239.1 has been modified.", SenderType="Management Server", EventId="8672153962696158442", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update", Result="Success", ObjectName="Firewall cPP Template"

FTA_TSE.1.1 TOE Session Establishment	
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	Sep 27 10:43:59 192.0.2.2 Timestamp="2022-09-27 10:43:59", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="8672153962696158444", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update", Result="Success", ObjectName="Firewall cPP Template"
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	Sep 27 10:43:59 192.0.2.2 Timestamp="2022-09-27 10:43:59", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="rule_validity_time_ref has been added: <rule_validity_time_ref type='rule_validity_time' value='Weekends'/>.", SenderType="Management Server", EventId="8672153962696158443", UserOriginator="root", ClientIpAddress="192.0.2.85", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Firewall cPP Template"

FAU_GEN.1/VPN Audit Data Generation (VPN Gateway)	
Auditable event	

FAU_GEN.1/VPN Audit Data Generation (VPN Gateway)	
Indication that TSF self-test was completed (NGFW)	Sep 29 07:22:59 192.0.2.1 Timestamp="2022-09-29 07:22:59", LogId="9995", NodeId="192.0.2.1", Facility="System Utilities", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="Thu Sep 29 07:22:10 2022 SHA512withECDSA checksum of the root file system succeed", ReceptionTime="2022-09-29 07:22:59", SenderType="Firewall", SituationId="73200", Situation="Self_Test-Success", EventId="6981106024069474059" Sep 29 07:22:59 192.0.2.1 Timestamp="2022-09-29 07:22:59", LogId="9996", NodeId="192.0.2.1", Facility="System Utilities", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="Thu Sep 29 07:21:38 2022 Cryptographic self-tests succeeded", ReceptionTime="2022-09-29 07:22:59", SenderType="Firewall", SituationId="73202", Situation="Self_Test-Cryptography-Success", EventId="6981106024069474060" Sep 29 07:23:00 192.0.2.1 Timestamp="2022-09-29 07:23:00", LogId="9998", NodeId="192.0.2.1", Facility="Management", Type="Notification", CompId="NGFW-FIPS node 1", InfoMsg="Thu Sep 29 07:22:09 2022 Integrity check: Engine image signature verified", ReceptionTime="2022-09-29 07:23:00", SenderType="Firewall", SituationId="73200", Situation="Self_Test-Success", EventId="6981106028364441358"
Indication that TSF self-test was completed (SMC)	Apr 2 16:02:45 127.0.0.1 Timestamp="2023-04-02 16:02:45", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Apr 2 16:00:15 smca root: fipscheck:Performing FIPS integrity check...",ReceptionTime="2023-04-02 16:02:45", SenderType="Third Party Device", EventId="2126"

FAU_GEN.1/VPN Audit Data Generation (VPN Gateway)	
Failure of self-test (NGFW)	`Sep 30 16:56:04 192.0.2.4 Timestamp="2022-09-30 16:56:04", LogId="1", NodeId="192.0.2.4", Facility="System Utilities", Type="System alert", CompId="NGFW node 1", InfoMsg="Fri Sep 30 16:54:24 2022 SHA512withECDSA checksum of the root file system failed", ReceptionTime="2022-09-30 16:56:04", SenderType="Firewall", SituationId="73201", Situation="Self_Test-Fail", AlertSeverity="Critical", EventId="6981612637205299201"`  `Sep 30 16:56:06 192.0.2.4 Timestamp="2022-09-30 16:56:06", LogId="159", NodeId="192.0.2.4", Facility="System Utilities", Type="System alert", CompId="NGFW node 1", InfoMsg="Fri Sep 30 16:54:25 2022 FIPS: rootfs integrity check FAILED rebooting...", ReceptionTime="2022-09-30 16:56:05", SenderType="Firewall", SituationId="73201", Situation="Self_Test-Fail", EventId="6981612641231831199"`

Failure of self-test (SMC)	`Apr  2 16:25:22 smca root: fipscheck:Performing FIPS integrity check...`
	
	`Apr  2 16:25:51 smca root: Fatal FIPS Error: fipscheck:ERROR:FIPS integrity check failed. /usr/bin/smca-fipscheck: 255`

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 NGFW 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.

Update Failures

The update process can fail for the following reasons:

- The digital signature verification fails for the update. When the signature verification fails the update is not imported. Therefore there is no need to remove the invalid update. Verify that the update is intended for the particular product component and version before importing it.
- The storage space is exceeded while importing the update. Take the following steps to remove any earlier updates that are no longer needed:
  - Select **Configuration**, then browse to **Administration**.
  - Browse to **Engine Updates**.
  - If there is any unnecessary imported **Engine Updates**, right-click it and select **Delete**.
  - Browse to **SMC Appliance Patches**.
  - If there is any unnecessary loaded patch, right-client it and select **Unload**.
  - Try to import the update again.

When upgrading the NGFW system to a newer major release, it is necessary to update the virtual SMC Appliance before the NGFW Engines. The order is not significant when applying maintenance release updates.

If an incorrect NGFW Engine version update was applied, you can revert to the previous installed NGFW Engine version. Restart the appliance and select the previous version from the boot menu on the appliance console.

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 (6.10.9P001.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/6.10.9P001.sap
```

5) Install the patch using the following command:

```
$ sudo ambr-install 6.10.9P001
```

6) Follow the instructions shown on the screen.

VPN Recovery Instructions

In case VPN connection does not work, recovery should start from investigating why VPN tunnel is not established. Examining logging in detail gives indication of the underlying problem. Basic steps to follow are described below.

Note

More detailed IPsec VPN messages will be logged after Diagnostics logging has been enabled for IPsec facility. To enable more detailed logging, right-click the NGFW Engine, select **Options** > **Diagnostics** then under **VPN**, select **IPsec VPN**. Click **OK** to close the dialog box.

- Check for certificate validity:
  - Verify that certificates of local or external VPN Gateway have not expired.
  - Verify that certificates of local or external VPN Gateway have not been revoked if revocation checking has been configured.
  - If revocation checking is configured, check that revocation information can be accessed.
- VPN negotiation issues:
  - IPsec VPN negotiation issues happen mostly between NGFW and external VPN Gateway tunnel negotiations due to mismatched definitions. The main thing to keep in mind when troubleshooting VPN negotiation issues is making sure settings match:
    - IKE version
    - IKE SA cipher algorithm
    - IKE SA message digest algorithm
    - IKE SA Diffie-Hellman group
    - IKE SA authentication method
    - IPsec SA type (ESP or AH)
    - IPsec SA cipher algorithm
    - IPsec SA message digest algorithm
    - IPsec SA compression algorithm (none or deflate)
    - IPsec SA granularity (SA per net or SA per host)
    - (Optional) IPsec SA Diffie-Hellman group if PFS is used
    - IPsec SA site definitions (traffic selectors / proxy IDs)
    - Trusted VPN Certificate Authority configuration
    - VPN endpoint identity configuration
      - Phase-1 ID Type and ID Value

If VPN negotiation fails, IPsec logs must be checked as the first step:

1) Log in to SMC using the Management Client or using SMC Web Access.

2) On the **Home** / **Dashboard** page right-click the firewall related to the **VPN problem** > **Monitoring** > **Logs by Sender**.

Note

If the VPN is failing between two NGFW engines managed by the same SMC, you can select both firewalls by holding the **Ctrl** button down.

3) In the **Logs** view **Query panel** use the drop-down menu to select **VPN**.

Note

If you do not see the **VPN** option, click the **Select** button, scroll down, click to select the **VPN**.

4) Click the **Apply** button on the **Query panel**.

5) (Optional) Add a filter as needed.

6) Check what logs (especially the **Information Message** field) indicate as the reason for the VPN failure.

When checking logs, keep in mind the following:

- You should have access to logs from both the gateways as IPsec standard does not permit sending exact error message to peer gateway.
- If NGFW logs show only generic No proposal chosen without more details, check logs from the External VPN Gateway as logging on that gateway will likely have more details.
- Each IPsec tunnel negotiation is composed of an initiator and a responder:
  - The initiator is the gateway which receives the traffic, i.e. traffic that should be sent through the tunnel, while the tunnel is not yet established, and thus initiated the negotiation.
  - The responder is the gateway which responds to a negotiation request from the peer (initiator) gateway.
  - Negotiation usually fails on the responder side.
- If NGFW is the initiator, and you do not have access to External VPN Gateway logs, try initiating new negotiation from the host behind the External VPN Gateway so that NGFW will be the responder, and thus more detailed error should be seen in the NGFW IPsec logs to which you have access.

Note

A mismatch in VPN settings might not trigger the same error when the initiator changes. If possible, when troubleshooting IPsec negotiation between NGFW and External VPN Gateway, try and access both the gateways' logs to see both perspectives.

After identifying the issue, adjust the configuration as needed.

- Refer to *VPN Certificates for VPN certificate management* section.
- Refer to *Create VPN Profile elements for VPN settings* section.

Refresh the policies of all firewalls involved in the VPN to activate the new configuration.

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.
/usr/local/forcepoint/smc/jre/bin/java	Management Server	8085/TCP	SMC Web Access clients	Ring 3	sgadmin	0	No	Communication for using SMC Web Access.
/usr/sbin/snmpd	SMC Appliance	161/UDP	Third-party components	Ring 3	snmp	0xffffffffffffffff=all	No	Requesting health and other information about the SMC Appliance.

Process	Listening	Ports/ Protocol	Contact-ing	Hardware Privilege	User	Linux Capabilities	TLS	Description
/usr/local/ forcepoint/ smc/jre/ bin/java	Syslog server	6514/TCP	Manage-ment Server, Log Server	Ring 3	sgadmin	0	Client	Audit and log data forwarding to syslog servers.
/usr/sbin/ snmpd	Third-party compon-ents	162/UDP	SMC Appliance	Ring 3	snmp	0xffffffffffffffff=all	No	Sending SNMP status probing to external devices.
/usr/local/ forcepoint/ smc/jre/ bin/java	Update servers	443/TCP	Manage-ment 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.

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	sgadmin	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	smonitd	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.

Process	Listening	Ports/ Protocol	Contact-ing	Hardware Privilege	User	Linux Capabilities	TLS	Description
/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	smonitd	0x0000003fffffffff	No	SNMP traps from the NGFW Engine.
/usr/sbin/ dnsmasq	Firewall	53/TCP, 53/UDP	Any	Ring 3	nobody	0x0000003fffffffff	No	DNS relay

Published 06 April 2023