



Network Security Platform

7.3.2

**Common Criteria Evaluated
Configuration Guide**

Contents

- [Introduction](#) on page 2
- [Evaluated capabilities](#) on page 3
- [How Security Engine process traffic](#) on page 5
- [Establishing a security configuration](#) on page 6
- [Secure the update process](#) on page 161
- [VPN Recovery Instructions](#) on page 162
- [Network processes](#) on page 164

Introduction

This guide describes the requirements and guidelines for configuring the Forcepoint Network Security Platform to comply with Common Criteria evaluation standards.

The system includes:

- Centralized management on the Forcepoint Network Security Platform Security Management Center Appliance (SMC Appliance) virtual appliance on ESXi 8.0 on Dell PowerEdge R440 with a pre-installed Management Server and Log Server.
- One or more Security Engines that run on pre-installed Security Engine appliances or Security Engine virtual appliances on ESXi 8.0 on Dell PowerEdge R440.

Evaluated products

The identification for the evaluated product is Forcepoint Network Security Platform 7.3.2.

The target of evaluation consists of:

- Forcepoint Network Security Platform Security Management Center Appliance (SMC Appliance) virtual appliance on ESXi 8.0 on Dell PowerEdge R440 with:
 - SMC Appliance software version 7.3.2
 - SMC FIPS Library 3.0.7 (based upon Oracle Linux 9 OpenSSL FIPS Provider 3.0.7-b27cdeb3ba51be46)
 - SMC FIPS Java API 2.0.1 (based upon BC-FJA (Bouncy Castle FIPS Java API) 2.0.1)
 - SMC FIPS Cryptographic Module for NTP 3.101.0 (based upon Oracle Linux 9 NSS Cryptographic Module 3.101.0)
- Security Engine with:
 - Security Engine software version 7.3.2
 - Forcepoint Network Security Platform FIPS Library 3.1.2 (based upon OpenSSL 3.1.2 FIPS)
 - Forcepoint Network Security Platform FIPS Cryptographic Module 2.0 (based upon SafeZone FIPS SW Cryptographic Module 2.0)
 - Forcepoint Network Security Platform Cryptographic Kernel Module 3.0

- Desktop appliance models: 60L, 61, 120, 120L, 120W, 120WL, 125L, 352, and 355.
- 1U appliance models: 1202, 2201, 2205, 2210, 2305, and 2310.
- 2U appliance models: 3401, 3405, 3505, and 3510
- Security Engine as a virtual machine on an ESXi 8.0 on Dell PowerEdge R440 server

**Note**

Cryptographic modules other than those listed above have not been evaluated nor tested during this Common Criteria evaluation.

Supporting documentation

These Forcepoint Network Security Platform documents are referenced throughout this guide.

- *Forcepoint Network Security Platform Product Guide*, version 7.3.0, revision A
- *Forcepoint Network Security Platform Installation Guide*, version 7.3.0, revision A

Evaluated capabilities

The Forcepoint Network Security Platform 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 traffic filtering firewall using Ethernet interfaces of Security Engine.
- IPSec VPN Gateway and headend functions

Forcepoint Network Security Platform

The Forcepoint Network Security Platform combines centralized management and firewalls into one platform. The system includes SMC user interface components, SMC server components, and Security Engines.

Component	Description
SMC Client	The SMC Client is the user interface for the SMC. The SMC Client version must match the version of the SMC.  Note The SMC Client is used to configure the Management Server and Log Server, but the SMC Client itself is not part of the target of evaluation. You use the SMC Client for all configuration and monitoring tasks. This interface allows the administrator to configure, monitor, and create reports about the whole Forcepoint Network Security Platform with the same tools and within the same user session. - You can install the SMC Client locally as an application, or you can login to the SMC Web Access management UI by using a web browser. - You can install an unlimited number of SMC Clients. - Multiple administrators can log on at the same time to efficiently configure and monitor all Security Engines.
SMC servers	SMC Appliance provides a unified hardware or virtual 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.
Security Engines	Security Engines inspect network traffic. The Security Engines software includes a purpose built operating system and there is no need for separate OS patches or upgrades. All software on Security Engines is updated during the software upgrade. The Engine policies determine when to use stateful connection tracking, packet filtering, or application-level security.

Certificates are validated as part of the authentication process when they are presented to the Forcepoint Network Security Platform and when they are loaded into the Forcepoint Network Security Platform. The following fields are verified as appropriate:

- signature
- validity period
- extended key usage
- issuer's name
- basic constraints (for CA certificates)

At import, the Forcepoint Network Security Platform also verifies that the certificate does not use explicit curve parameters and that the certificate chains to a valid CA certificate.

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 Security 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 Security 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 Security Engine process traffic

Security Engines permit or deny traffic according to Engine filtering rules that are contained in an Engine Policy. Rules match based on administrator defined properties of the traffic and the interface.

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

Access rules are traffic handling rules that define how the traffic is examined and what action the Security 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 Network Security Platform Product Guide*.

Network packets are accepted automatically without additional processing when connection tracking is enabled. When Strict connection tracking mode is used, the Security 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.

Security Engine supports several protocols and their attributes in a Engine policy. The protocols listed in the table are supported. Within each protocol, certain attributes are subject to Engine 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

Protocol	Attributes used for matching
RFC 2460 (IPv6)	■ Source address ■ Destination address ■ Transport layer protocol
RFC 793 (TCP)	■ Source port ■ Destination port
RFC 768 (UDP)	■ Source port ■ Destination port

**Note**

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

**Note**

TCP traffic on port 21 is by default interpreted as FTP protocol (RFC 959) traffic. If this control connection is allowed by Access rules and traffic on port 21 contains valid FTP protocol commands to open a data connection, the Security 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 Network Security Platform Product Guide*.

For more information about dynamic session establishment capabilities, see the *Support for multi-layer inspection* topic in the *Introduction to Forcepoint Network Security Platform in the Engine/VPN role* chapter in the *Forcepoint Network Security Platform Product Guide*.

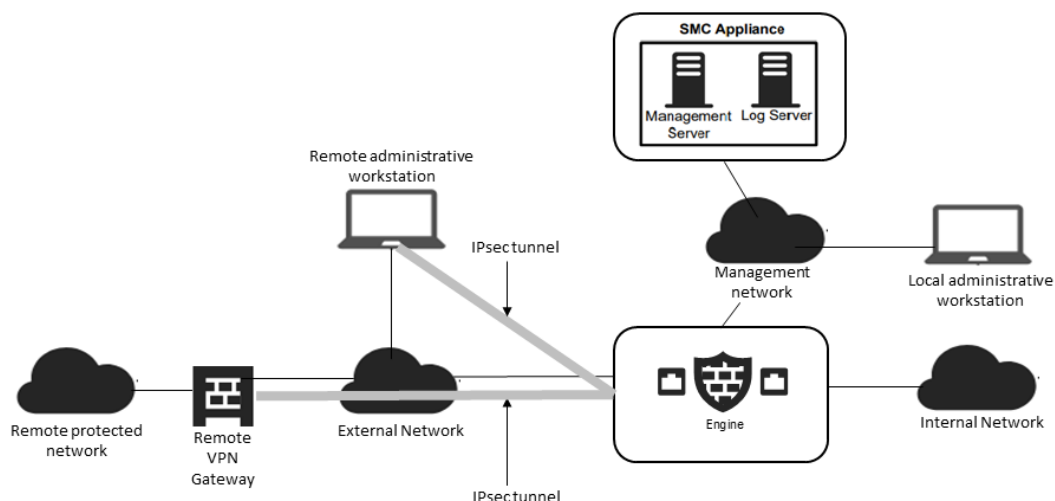
Establishing a security configuration

A Common Criteria configuration that also meets IPsec VPN gateway requirements for Commercial Solutions for Classified (CSfC) solutions program requires a specific configuration of the SMC Appliance, SMC software, and Security Engines.

**Note**

When a CSfC compliant configuration requires specific selections for setup, those requirements are noted separately.

Components overview



Preparations for the configuration

- Install the Forcepoint Network Security Platform components within a physically protected environment.
- The Forcepoint Network Security Platform is administered over a trusted and separate management network.
- Multiple installations of the Security Engine may be used in combination.
- Connect the Virtual SMC Appliance and Security Engines to the management network using dedicated management network interfaces.
- Connect the Security Engines to the internal and external networks.
- The evaluated configuration includes a virtualization server or virtualization servers where the Virtual SMC Appliance and Virtual Security Engine are run as 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 Security Engine 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) Perform the initial SMC configuration that includes setting the IP address, initial administrator account creation, and certificate enrollment with an external Certificate Authority.

- 4) Install the SMC Client, then configure the security parameters for the Common Criteria evaluated configuration.
- 5) Create and install Security Engines in FIPS mode. The Security Engine appliance runs a series of self-tests.
- 6) If the Security Engine appliance self-tests result in errors, reset the appliance to factory settings.
- 7) Enroll Security Engines with an external Certificate Authority to establish secure management communication with the SMC.
- 8) Review the audit events.

FIPS mode restrictions

When FIPS mode is enabled, the following restrictions are enforced:

- The Security 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

Additionally, when the management server, log server, and security engines are enrolled with an ECDSA key size of 384 bits (NIST curve P-384), the following additional restrictions are implicitly enabled:

- When SMC or Security Engine acts as the TLS client, the supported signature algorithms in the TLS signature_algorithms extension for management connections are limited to ecdsa_secp384r1_sha384 (0x0503).
- When SMC acts as the TLS client, the supported groups in the TLS supported_groups extension for management connections are limited to secp384r1 (0x0018).
- When SMC or Security Engine acts as the TLS server, the signature algorithms in the certificate request for management connections are limited to ecdsa_secp384r1_sha384 (0x0503).

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 8.0. Follow the guidelines in the Installing SMC Appliance software on a virtualization platform appendix in the *Forcepoint Network Security Platform Installation Guide*.



Note

- The ESXi host must have the hardware entropy pass-through enabled for both the SMC and the Engine.
- According to the VMware [Controlling ESXi Entropy](#), FIPS entropy handling is the default behavior if the following conditions are true:
 - The hardware supports RDSEED.
 - The disableHwrng VMkernel boot option isn't present or is FALSE.
 - The entropySources VMkernel boot option isn't present, is 0 (zero), or is 4.

- 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 with SHA-512 in digital signatures for the Common Criteria evaluated configuration in connections between the SMC and the Security Engines.



Note

ECDSA P-384 with SHA-384 for the Commercial Solutions for Classified configuration.

- P-521 NIST curve for the Common Criteria evaluated configuration in TLS key establishment in connections between the SMC and the Security Engines. .



Note

P-384 NIST curves for the Commercial Solutions for Classified configuration.

- P-256, P-384, and P-521 NIST curves, in TLS key establishment, with SHA-256, SHA-384, or SHA-512 in digital signatures, in Web Access and in connections to external servers.

The Management Server and Log Server only accepts the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suites when acting as TLS server for connections from Security Engines.

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

Steps

- 1) After SMC Appliance reboots following the installation, please proceed by accepting the End User License Agreement (EULA).
- 2) Select **Begin**, then press **Enter**.
- 3) Select the keyboard layout for accessing the SMC Appliance on the command line.
- 4) Enter the administrator account name and password.



Note

The administrator account and password are used for command line access to the SMC Appliance and for access to the SMC Client. The administrator account is created with unrestricted permissions (superuser).

- a) Enter the account name.
This field is case sensitive and limited to eight characters.
 - b) Enter the password.
The password is case sensitive. The password must be at least ten characters long and contain at least one number.
 - c) Enter the password again.
- 5) (Optional) Configure a bootloader password.
If you configure a bootloader password, you must enter the bootloader password to edit the options that appear in the bootloader menu of the SMC Appliance.
 - a) Press the space bar to configure a bootloader password.
 - b) Enter the password.
 - c) Enter the password again.
 - 6) Make your security selections.
 - a) Select FIPS mode.
 - b) Select 256-bit encryption as the security strength.

c) Select Use External Certificate Authority.

**Note**

- When you install the SMC, you can use certificates issued by an external CA for internal TLS communication between system components.
- Using certificates issued by an external CA allows you to use your own established internal CA infrastructure to generate certificates for communication between components. Certificate revocation checking is also supported. If any devices are compromised, the certificates associated with them can be revoked and replaced centrally using the external certificate management system.
- When using external certificates:
 - You can only configure the SMC to use external certificates when you install the SMC. It is not possible to change to using external certificates in an existing installation.
 - To use certificate revocation lists (CRLs) or online certificate status protocol (OCSP) servers, you must configure a DNS server.
 - The Management Server and Log Server services do not start immediately after installation because the components do not yet have certificates.
 - You must complete the following actions after installation before you can start using the SMC:
 - Import the external CA certificate.
 - Generate and export certificate requests.
 - Sign the certificates using the external CA.
 - Import the signed certificates.

**Note**

Only the ECDSA public key algorithm is supported.

- 7) To enable network interface configuration, select **Disabled**, then press **Enter**.
- 8) Complete the network interface configuration for the primary network interface for management.
 - a) Select **Enable interface**.
 - b) Select **Primary**.
 - c) Complete the network configuration fields for the interface.
- 9) (Optional) Complete the network interface configuration for the secondary network interface for management.
 - a) Select **Enable interface**.
 - b) Select **Secondary**.
 - c) Complete the network configuration fields for the interface.

- 10) Enter a host name for the Management Server.
- 11) (Optional) Enter one or more IPv4 or IPv6 addresses in the DNS server fields.

**Note**

When using an external CA, it is necessary to configure at least one DNS server.

- 12) (Optional) If you do not want to use NTP, disable it in the NTP settings.

**Note**

We recommend that you configure an NTP server so that the time settings for the SMC are accurate when checking validity times for certificates, CRLs, and OSCP server responses.

- 13) Select the time zone.
- 14) Set the date and time.
You are prompted to review the configuration.
- 15) Select **Confirm**, then press **Enter**.

Result

When the installation is complete, select one of the following options:

- Reboot
- Shutdown.

External SMC certificate management configuration overview

When you use external certificate management, the SMC configuration consists of these general tasks.

- 1) Create a certificate for the Management Server.
- 2) Create a certificate for the Log Server.
- 3) Create certificates for Security Engines.

Create a certificate for the Management Server using external certificate management

Create a certificate request for the Management Server, export and sign the certificate request using the external CA, then import the signed certificate for the Management Server.

Steps

- 1) Log in to the console with the user account created during the installation.

- 2) Create a certificate signing request for the Management Server.

Enter the following command to create certificate request to the `/tmp/mgmt.csr` file:

```
sudo /usr/local/forcepoint/smc/bin/sgCertifyMgtSrv.sh mode=ext-pki-init key-size=384
dn="CN=MyMgmt,C=US,OU=MyCompany" dns="my-mgmt" csr-out=/tmp/mgmt.csr
```



Note

Key-size parameter of 521 bits is also acceptable if the configuration is not intended to be compatible with Commercial Solutions for Classified configuration.



Important

- Replace the 'dn' field value with an appropriate descriptive distinguished name for your environment.
- Replace the 'dns' field value with a suitable and unique domain name that identifies the management server in your environment.
- The CSfC compatible configuration can be disabled by generating a new Management Server certificate with a key size parameter of 521. The new configuration will then be Common Criteria compatible instead.

- 3) Export the generated CSR using scp.

Enter the following command:

```
scp /tmp/mgmt.csr <user>@<host>:<path>
```

- 4) Sign the CSR externally and import the certificates using scp. Any intermediate certificates must be bundled into the same file with the signed leaf certificate.

Enter the following command:

```
scp <user>@<host>:<path>/mgmt.cert.pem /tmp/
chmod a+r /tmp/mgmt.cert.pem
scp <user>@<host>:<path>/ca.cert.pem /tmp/
chmod a+r /tmp/ca.cert.pem
sudo /usr/local/forcepoint/smc/bin/sgCertifyMgtSrv.sh mode=ext-pki-import crt-in=/
tmp/mgmt.cert.pem ca-file=/tmp/ca.cert.pem
```

- 5) Start the Management Server.

Enter the following command:

```
sudo daemon-ctl restart sgMgtServer
```

Next steps

Install the SMC Client, and then create a certificate for the Log Server.

**Important**

- Installing the SMC Client is optional. You can access SMC by using SMC Web Access or by installing the SMC Client to a separate host. By default, the SMC Web Access is enabled when the management server starts.
- The SMC Client can be accessed using a web browser on https port 8085 on the SMC Appliance. For example, if the SMC Appliance is configured with the IP address 192.0.2.1, the SMC Client can be accessed using the URL https://192.0.2.1:8085/ in a web browser.

Renew a certificate for the Management Server

You must renew the external certificate before it expires.

Steps

- 1) Log in to the console with the user account created during the installation.

- 2) Stop the Management Server.

Enter the following command to stop the Management Server:

```
sudo daemon-ctl stop sgMgtServer
```

- 3) Create a new certificate request.

Enter the following command to create a new certificate request:

```
sudo /usr/local/forcepoint/smc/bin/sgCertifyMgtSrv.sh -reinit mode=ext-pki-init key-size=384
dn="CN=MyMgmt,
C=US,OU=MyCompany" dns="my-mgmt" csr-out=/tmp/mgmt.csr
```

**Note**

Key-size parameter of 521 bits is also acceptable if the configuration is not intended to be compatible with Commercial Solutions for Classified configuration.

**Important**

- Replace the 'dn' field value with an appropriate descriptive distinguished name for your environment.
- Replace the 'dns' field value with a suitable and unique domain name that identifies the management server in your environment.
- The CSfC compatible configuration can be disabled by generating a new Management Server certificate with a key size parameter of 521. The new configuration will then be compatible with CC instead.

- 4) Export the generated CSR using scp.

Enter the following command:

```
scp /tmp/mgmt.csr <user>@<host>:<path>
```

- 5) Sign the CSR externally and import the certificates using scp. Any intermediate certificates must be bundled into the same file with the signed leaf certificate.

Enter the following command:

```
scp <user>@<host>:<path>/mgmt.cert.pem /tmp/
chmod a+r /tmp/mgmt.cert.pem
scp <user>@<host>:<path>/ca.cert.pem /tmp/
chmod a+r /tmp/ca.cert.pem
sudo /usr/local/forcepoint/smc/bin/sgCertifyMgtSrv.sh mode=ext-pki-import crt-in=/
tmp/mgmt.cert.pem ca-file=/tmp/ca.cert.pem
```

- 6) Start the Management Server.

Enter the following command:

```
sudo daemon-ctl restart sgMgtServer
```

Next steps

Install the SMC Client, and then create a certificate for the Log Server.



Important

- Installing the SMC Client is optional. You can access SMC by using SMC Web Access or by installing the SMC Client to a separate host. By default, the SMC Web Access is enabled when the management server starts.
- The SMC Client can be accessed using a web browser on https port 8085 on the SMC Appliance. For example, if the SMC Appliance is configured with the IP address 192.0.2.1, the SMC Client can be accessed using the URL https://192.0.2.1:8085/ in a web browser.

Install the SMC Client

Optionally you can install a stand-alone SMC Client application in FIPS mode on a Windows or Linux workstation. For system requirements, see the SMC release notes for your version.

As an alternative to installing the SMC Client, you can use Web Access.

When logging on to the SMC Client, the fingerprint of the Management Server certificate is verified.

Steps

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

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

Decompress the .zip file.

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

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

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

- 3) Select the language for the installation, then click **OK**.
The language that you select is also set as the default language of the SMC Client.
- 4) Read the information on the **Introduction** page, then click **Next**.

**Tip**

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

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

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

The default installation directory in Windows is `C:\Program Files\Fortinet\Fortinet` and in Linux is `/usr/local/fortinet/smc`. Click **Choose** to browse to a different installation folder.

**Note**

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

- 7) (Linux only) Read the instructions about the hosts file, make any necessary configuration changes, then click **Next**.
- 8) Select where to create shortcuts, then click **Next**.
These shortcuts can be used to manually start components and to run some maintenance tasks.
- 9) Select **SMC Client Only** as the installation type, then click **Next**.
- 10) When prompted to select the cryptographic algorithms, select **Restricted Cryptographic Algorithms Compatible with FIPS**.
- 11) Click **Next** to continue to the Pre-Installation Summary.

**Important**

In the Pre-Installation Summary the user can review the installation settings. Click **Previous** to adjust your selections.

- 12) Click **Install** to begin the installation.
- 13) When the installation has completed, click **Done**.

Create a certificate for the Log Server using external certificate management

Create a certificate request for the Log Server, export and sign the certificate request using the external CA, then import the signed certificate for the Log Server.

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

- 1) Start the SMC Client.
- 2) Accept the Management Server certificate. A certificate dialog box containing the Management Server certificate fingerprint is shown when the SMC Client contacts a Management Server for the first time. Confirm that the fingerprint shown on the client matches the server certificate fingerprint.
 - a) To view the Management Server certificate fingerprint, log on to the SMC Appliance command line with your administrator credentials, then run the following command:

```
sudo smca-system fingerprint
```

- b) If the fingerprint shown on the command line matches the one in the client dialog box, click **Accept**.
- 3) Complete the certificate request details for the Log Server.
 - a) Select  **Dashboard > Servers / Devices Dashboard**.
 - b) Browse to **Log Server**.
 - c) Right-click the Log Server, then select **Properties**.
 - d) On the **Certificate** tab, enter the following information:
 - **Common Name (CN)** — Enter a common name that includes the name of the Log Server element.
 - **Subject Alternative Name (DNS)** — Enter the name of the Log Server as a fully qualified domain name (FQDN).



Note

The value of the **Subject Alternative Name (DNS)** must be unique within the SMC and the external CA.

- **Key Length** — Select 384.



Note

Key-size parameters of 521 bits is also acceptable if the configuration is not intended to be compatible with Commercial Solutions for Classified configuration.

- e) Complete the other certificate request details according to your environment.
 - f) Click **OK** to close the Log Server Properties dialog box.

- 4) On the command line of the SMC Appliance, create a certificate request and a private key for the Log Server.
 - a) Enter the `sgCertifyLogSrv` command:

```
sudo /usr/local/forcepoint/smc/bin/sgCertifyLogSrv.sh
```
 - b) Enter the credentials for an administrator account with unrestricted permissions (superuser).
When the certification has finished, a certificate request is created for the Log Server.
- 5) In the SMC Client, export the certificate request.
 - a) Select  **Dashboard > Servers / Devices Dashboard**.
 - b) Browse to **Log Server**.
 - c) Right-click the Log Server, then select **Properties**.
 - d) On the **Certificate** tab, click **Export Certificate Request**, browse to the location where you want to save the certificate request, then click **Save**.
Save the certificate request in a location that is accessible from your local workstation.
 - e) Click **OK** to close the Export Certificate dialog box.
 - f) Click **OK** to close the Log Server Properties dialog box.
- 6) Sign the certificate request using the external CA, then copy the signed certificate to a location that is accessible from your local workstation.
- 7) In the SMC Client, import the signed certificate for the Log Server.
 - a) Select  **Dashboard > Servers / Devices Dashboard**.
 - b) Browse to **Log Server**.
 - c) Right-click the Log Server, then select **Properties**.
 - d) On the **Certificate** tab, click **Import Signed Certificate**.
 - e) Browse to the signed certificate file, then click **OK**.
 - f) Click **OK** to close the Log Server Properties dialog box.
- 8) On the command line of the SMC Appliance, transfer the signed certificate to the Log Server.
 - a) Enter the `sgCertifyLogSrv` command:

```
sudo /usr/local/forcepoint/smc/bin/sgCertifyLogSrv.sh
```
 - b) Enter the credentials for an administrator account with unrestricted permissions (superuser).

9) Start the Log Server.

Enter the following command on SMC Appliance:

```
sudo daemon-ctl restart sgLogServer
```

Log Server Properties dialog box - Certificate tab

Option	Definition
Current Certificate	Shows information about the current certificate of the server. Click Export Certificate to export the current certificate. Click Renew Certificate to renew the certificate.
Check Revocation	Checks against certificate revocation lists (CRLs or OCSP) whether the certificate of the new connection has been revoked. The certificate must be signed by a valid certificate authority.
Ignore Revocation Check Failures if There Are Connectivity Problems	When selected, the server ignores all CRL check failures if the server cannot connect to CRL or OCSP server. This is done based on what is specified in the certificate.
Organization (O) (Optional)	The name of your organization as it appears in the certificate.
Organization Unit (OU) (Optional)	The name of your department or division as it appears in the certificate.
State/Province (ST) (Optional)	The name of state or province as it appears in the certificate.
Locality (L) (Optional)	The name of the city as it appears in the certificate.
Common Name (CN)	A common name that includes the name of the Log Server element.
Public Key Algorithm (Not editable)	The algorithm used for the public key.  Note For Log Server certificates, only the ECDSA public key algorithm is supported.
Key Length	The length of the key in bits. Select 384.  Note Key-size parameter of 521 bits is also acceptable if the configuration is not intended to be compatible with Commercial Solutions for Classified configuration.
Signature Algorithm (Not editable)	Shows the signature algorithm according to the key length.
Subject Alternative Name (DNS)	Name of the Log Server as a fully qualified domain name (FQDN).
Generate Certificate Request	Shows the certificate request as text.
Export Certificate	Exports the certificate request so that you can sign it using an external certificate authority.

Option	Definition
Import Signed Certificate	Imports a certificate that has been signed using an external certificate authority.

Next steps

Create Security Engine elements, then create certificates for the Security Engines.

Renew a certificate for the Log Server

You must renew the external certificate before it expires. If the certificate has expired or has been revoked a new certificate request must be generated.

Steps

1) Do one of the following:

- If the current certificate is still valid:
 - a) Start the SMC Client.
 - b) Select  **Dashboard > Servers / Devices Dashboard**.
 - c) Browse to **Log Server**.
 - d) Right-click the Log Server, then select **Properties**.
 - e) On the **Certificate** tab, do the following:
 - i) Verify the information in the **Certificate Definition** Section.
 - ii) Click **Generate Certificate Request**.

- If the current certificate has expired or has been revoked:



Note

This needs to be done from the command line of the SMC Appliance.

- a) Start the SMC Client.
- b) Stop the Log Server.
Enter the following command:


```
sudo daemon-ctl stop sgLogServer
```
- c) Generate a new CSR for the Log Server.
Enter the following command:


```
sudo /usr/local/forcepoint/smc/bin/sgCertifyLogSrv.sh -reinit
```
- d) Enter the credentials for an administrator account with unrestricted permissions (superuser). When the certification has finished, a certificate request is created for the Log Server.

2) In the SMC Client, export the certificate request.

- a) Select  **Dashboard > Servers / Devices Dashboard**.
- b) Browse to **Log Server**.
- c) Right-click the Log Server, then select **Properties**.

- d) On the **Certificate** tab, click **Export Certificate Request**, browse to the location where you want to save the certificate request, then click **Save**.
Save the certificate request in a location that is accessible from your local workstation.
 - e) Click **OK** to close the Export Certificate dialog box.
 - f) Click **OK** to close the Log Server Properties dialog box.
- 3) Sign the certificate request using the external CA, then copy the signed certificate to a location that is accessible from your local workstation.
 - 4) In the SMC Client, import the signed certificate for the Log Server.
 - a) Select **Dashboard > Servers / Devices Dashboard**.
 - b) Browse to **Log Server**.
 - c) Right-click the Log Server, then select **Properties**.
 - d) On the **Certificate** tab, click **Import Signed Certificate**.
 - e) Browse to the signed certificate file, then click **OK**.
 - f) Click **OK** to close the Log Server Properties dialog box.
 - 5) On the command line of the SMC Appliance, transfer the signed certificate to the Log Server.
 - a) Enter the `sgCertifyLogSrv` command:


```
sudo /usr/local/forcepoint/smc/bin/sgCertifyLogSrv.sh
```
 - b) Enter the credentials for an administrator account with unrestricted permissions (superuser).
 - 6) Start the Log Server.
Enter the following command on SMC Appliance:

```
sudo daemon-ctl restart sgLogServer
```

Log Server Properties dialog box - Certificate tab

Option	Definition
Current Certificate	Shows information about the current certificate of the server. Click Export Certificate to export the current certificate. Click Renew Certificate to renew the certificate.
Check Revocation	Checks against certificate revocation lists (CRLs or OCSP) whether the certificate of the new connection has been revoked. The certificate must be signed by a valid certificate authority.

Option	Definition
Ignore Revocation Check Failures if There Are Connectivity Problems	When selected, the server ignores all CRL check failures if the server cannot connect to CRL or OCSP server. This is done based on what is specified in the certificate.
Organization (O) (Optional)	The name of your organization as it appears in the certificate.
Organization Unit (OU) (Optional)	The name of your department or division as it appears in the certificate.
State/Province (ST) (Optional)	The name of state or province as it appears in the certificate.
Locality (L) (Optional)	The name of the city as it appears in the certificate.
Common Name (CN)	A common name that includes the name of the Log Server element.
Public Key Algorithm (Not editable)	The algorithm used for the public key.  Note For Log Server certificates, only the ECDSA public key algorithm is supported.
Key Length	The length of the key in bits. Select 384.  Note Key-size parameter of 521 bits is also acceptable if the configuration is not intended to be compatible with Commercial Solutions for Classified configuration.
Signature Algorithm (Not editable)	Shows the signature algorithm according to the key length.
Subject Alternative Name (DNS)	Name of the Log Server as a fully qualified domain name (FQDN).
Generate Certificate Request	Shows the certificate request as text.
Export Certificate	Exports the certificate request so that you can sign it using an external certificate authority.
Import Signed Certificate	Imports a certificate that has been signed using an external certificate authority.

Next steps

Create Security Engine elements, then create certificates for the Security Engines.

Create certificates for Security Engines using external certificate management

After creating an Security Engine element, create a certificate request for each Security Engine node, export and sign the certificate request using the external CA, then import the signed certificate.

Before you begin

Create an Security Engine element. For details, refer to the *Create an element for the Security Engine* topic in the *Forcepoint Network Security Platform Common Criteria Evaluated Configuration Guide*.

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

- 1) In the SMC Client, edit the certificate settings for each Security Engine node.
 - a) Select  **Engine Configuration**.
 - b) Right-click an engine, then select **Edit <element type>**.
 - c) Open the certificate settings in one of the following ways:
 - For single Security Engines, click **Certificate Settings** on the **General** tab of the Engine Editor.
 - For Security Engine clusters, browse to **General > Clustering**, right-click the **Certificate** cell for a node, then select **Edit Certificate**.
 - d) In the **Certificate Settings** dialog box, do the following:
 - Select the **Check Revocation** checkbox.
 - Make sure that the **Ignore Revocation Check Failures if There Are Connectivity Problems** checkbox is not selected.
 - **Common Name (CN)** — Enter a common name that includes the name of the Security Engine element.
Example: Helsinki Security Engine
 - **Subject Alternative Name (DNS)** — Enter the name of the Security Engine node as a fully qualified domain name (FQDN).
Examples:
helsinki-security-engine.example.com
helsinki-security-engine-node1.example.com



Note

The value of the **Subject Alternative Name (DNS)** must be unique within the SMC and the external CA.

- **Key Length** — Select 384.



Note

Key-size parameter of 521 bits is also acceptable if the configuration is not intended to be compatible with Commercial Solutions for Classified configuration.

- e) Complete the other certificate request details according to your environment.
 - f) Click **OK**.
- 2) Save the initial configuration for the Security Engine.
Follow the instructions in *Prepare for Security Engine Configuration Wizard configuration*.
 - 3) On the command line of the Security Engine, make initial contact between the Security Engine and the Management Server.
Follow the instructions in *Contact the Management Server on the command line*.
A certificate request is created for the Security Engine and transferred to the Management Server.
 - 4) In the SMC Client, export the certificate request for the Security Engine.
 - a) Select  **Engine Configuration**.
 - b) Right-click an Security Engine node, then select **Certificate > Export Certificate Request**.
 - c) Browse to the location to save the certificate request and name it as you want, then click **Export**.
 - d) Click **OK** to close the Certificate dialog box.
 - 5) Sign the certificate request using the external CA, then copy the signed certificate to a location that is accessible from your local workstation.
 - 6) In the SMC Client, import the signed certificate for the Security Engine.
 - a) Select  **Engine Configuration**.
 - b) Right-click an Security Engine node, then select **Certificate > Import Signed Certificate**.
 - c) Browse to the signed certificate file, then click **Import**.
 - d) Click **OK** to close the Import Certificate dialog box.



Note

Engine polls SMC for the certificate periodically. After Engine sees imported certificate from SMC, it fetches the certificate and then automatically reboots to activate the new certificate.

Result

The Security Engine node receives the signed certificate from the Management Server.

Certificate Settings dialog box

Option	Definition
Name	The name of the element.

Option	Definition
Organization (O) (Optional)	The name of your organization as it appears in the certificate.
Organization Unit (OU) (Optional)	The name of your department or division as it appears in the certificate.
State/Province (ST) (Optional)	The name of state or province as it appears in the certificate.
Locality (L) (Optional)	The name of the city as it appears in the certificate.
Common Name (CN)	A common name that includes the name of the Security Engine element.
Public Key Algorithm (Not editable)	The algorithm used for the public key.  Note For Security Engine certificates, only the ECDSA public key algorithm is supported.
Key Length	The length of the key in bits. Select 384.  Note Key-size parameter of 521 bits is also acceptable if the configuration is not intended to be compatible with Commercial Solutions for Classified configuration.
Signature Algorithm (Not editable)	Shows the signature algorithm according to the key length.
Subject Alternative Name (DNS)	The name of the Security Engine node as a fully qualified domain name (FQDN).

Renew a certificate for the Security Engine

You must renew the external certificate before it expires.

Steps

- 1) In the SMC Client, edit the certificate settings for each Security Engine node.
 - a) Select  **Engine Configuration**.
 - b) Right-click an engine, then select **Edit <element type>**.
 - c) Open the certificate settings in one of the following ways:
 - For single Security Engines, click **Certificate Settings** on the **General** tab of the Engine Editor.
 - For Security Engine clusters, browse to **General > Clustering**, right-click the **Certificate** cell for a node, then select **Edit Certificate**.

- 2) In the **Certificate Settings** dialog box, do the following:
 - a) Verify the information in the **Certificate Definition** Section.
 - b) Click **Generate Certificate Request**.
- 3) Browse to the location to save the certificate request and name it as you want, then click **Export**.
- 4) Click **OK** to close the Certificate dialog box.
- 5) Sign the certificate request using the external CA, then copy the signed certificate to a location that is accessible from your local workstation.
- 6) In the SMC Client, import the signed certificate for the Security Engine.
 - a) Select **Engine Configuration**.
 - b) Right-click an Security Engine node, then select **Certificate > Import Signed Certificate**.
 - c) Browse to the signed certificate file, then click **Import**.
 - d) Click **OK** to close the Import Certificate dialog box.



Note

Engine polls SMC for the certificate periodically. After Engine sees imported certificate from SMC, it fetches the certificate and then automatically reboots to activate the new certificate.

Verify the SMC Appliance self-tests

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

Known answer tests (KAT) and pairwise consistency tests (PCT) are run for the software cryptographic modules.

Integrity check verifies the ECDSA signature of a catalog file of the SHA-256 hashes of all binaries.

Noise source health tests include a Repetition Count Test and a Chi-Squared test to fulfill the role of the Adaptive Proportion Test as specified by NIST SP 800-90B.

SMC FIPS Java API self-tests

Algorithm	Type	Test Method
HMAC-SHA2-256	Software Integrity	Message Authentication
AES-ECB Encryption	CAST	KAT
AES-ECB Decryption	CAST	KAT
AES-CCM Encryption	CAST	KAT
AES-CCM Decryption	CAST	KAT
AES-CMAC Generation	CAST	KAT
AES-CMAC Verification	CAST	KAT

Algorithm	Type	Test Method
KAS-ECC Primitive “Z” Computation	CAST	KAT
KAS-FFC Primitive “Z” Computation	CAST	KAT
HASH_DRBG SHA2-256	CAST	KAT
HMAC-DRBG HMAC-SHA2-256	CAST	KAT
CTR_DRBG AES-CTR 256 bits	CAST	KAT
DSA Signature Generation	CAST	KAT
DSA Signature Verification	CAST	KAT
ECDSA Signature Generation	CAST	KAT
ECDSA Signature Verification	CAST	KAT
AES-GCM Encrypt	CAST	KAT
AES-GCM Decrypt	CAST	KAT
HMAC-SHA2-256	CAST	KAT
HMAC-SHA2-512	CAST	KAT
HMAC-SHA3-256	CAST	KAT
KDA OneStep	CAST	KAT
KDA TwoStep	CAST	KAT
KBKDF	CAST	KAT
PBKDF	CAST	KAT
SHA-3	CAST	KAT
RSA Signature Generation	CAST	KAT
RSA Signature Verification	CAST	KAT
RSA Encryption	CAST	KAT
RSA Decryption	CAST	KAT
SHA-1	CAST	KAT
SHA2-256	CAST	KAT
SHA2-512	CAST	KAT
SHAKE256	CAST	KAT
ANS 9.63 KDF	CAST	KAT
IKEv2 KDF	CAST	KAT
SNMP KDF	CAST	KAT
SRTP KDF	CAST	KAT
SSH KDF	CAST	KAT

Algorithm	Type	Test Method
TLS 1.0 KDF	CAST	KAT
TLS 1.1 KDF	CAST	KAT
TLS 1.2 KDF	CAST	KAT
HMAC	CAST	KAT
SHS	CAST	KAT
DH	Pair-Wise Consistency Test	PCT
DSA	Pair-Wise Consistency Test	PCT
EC DH	Pair-Wise Consistency Test	PCT
ECDSA	Pair-Wise Consistency Test	PCT
RSA	Pair-Wise Consistency Test	PCT

SMC FIPS Library self-tests

Algorithm	Type	Test Method
HMAC-SHA2-256	Software integrity	Message Authentication
SHA2-512	CAST	KAT
SHA3-256	CAST	KAT
AES-ECB	CAST	KAT
AES-GCM	CAST	KAT
KBKDF	CAST	KAT
KDA OneStep	CAST	KAT
HKDF	CAST	KAT
ANS X9.42 KDF (CVL)	CAST	KAT
ANS X9.63 KDF (CVL)	CAST	KAT
SSH KDF (CVL)	CAST	KAT
TLS 1.2 KDF (CVL)	CAST	KAT
TLS 1.3 KDF (CVL)	CAST	KAT
PBKDF2	CAST	KAT
CTR_DRBG	CAST	KAT
Hash_DRBG	CAST	KAT
HMAC_DRBG	CAST	KAT
KAS-FFC-SSC	CAST	KAT
KAS-ECC-SSC	CAST	KAT
RSA	CAST	KAT
ECDSA	CAST	KAT
ECDSA	Pair-Wise Consistency Test	PCT
RSA	Pair-Wise Consistency Test	PCT

Algorithm	Type	Test Method
Safe Primes	Pair-Wise Consistency Test	PCT

SMC FIPS Cryptographic Module for NTP self-tests

Algorithm	Type	Test Method
HMAC-SHA-256	Software integrity	Message Authentication
SHA-1	CAST	KAT
SHA-224	CAST	KAT
SHA-256	CAST	KAT
SHA-384	CAST	KAT
SHA-512	CAST	KAT
AES-ECB	CAST	KAT
AES-CBC	CAST	KAT
AES-GCM	CAST	KAT
AES-CMAC	CAST	KAT
HMAC SHA-224	CAST	KAT
HMAC SHA-256	CAST	KAT
HMAC SHA-384	CAST	KAT
HMAC SHA-512	CAST	KAT
KBKDF	CAST	KAT
HKDF	CAST	KAT
TLS 1.0/1.1 KDF	CAST	KAT
TLS 1.2 KDF	CAST	KAT
IKEv2 PRF	CAST	KAT
PBKDF2	CAST	KAT
Hash_DRBG	CAST	KAT
KAS-FFC-SSC	CAST	KAT
KAS-ECC-SSC	CAST	KAT
RSA	CAST	KAT
DSA	CAST	KAT
ECDSA	CAST	KAT
Safe Primes	Conditional Pairwise Consistency Self-Test	PCT
ECDH	Conditional Pairwise Consistency Self-Test	PCT
RSA	Conditional Pairwise Consistency Self-Test	PCT
ECDSA	Conditional Pairwise Consistency Self-Test	PCT

Check the self-test results in the console. The self-test messages are also sent to the SMC Appliance syslog.

- If the SMC FIPS Java API cryptographic module self-test fails, the server application fails to start, and an error message is shown on the console and the appliance halts its execution automatically.

```
fipssmc: ERROR: FIPS SMC Bouncy Castle
fipssmc: FIPS System Shutdown
```

- If a power-up self-test fails, an error message is shown on the console and the appliance halts and is not remotely accessible.

```
fipstest:Performing FIPS NSS crypto selftests...
Fatal FIPS Error: fipstest:ERROR:FIPS NSS crypto selftest failed: /lib/fips/fipstest-openssl: 255
```

```
fipstest: Performing FIPS OpenSSL crypto selftests...
Fatal FIPS Error: fipstest:ERROR:FIPS OpenSSL crypto selftest failed: /lib/fips/fipstest-openssl: 1
```

- If the file system integrity check fails, an error message is shown on the console and the appliance halts and is not remotely accessible.

```
fipscheck: Performing FIPS integrity check...
Fatal FIPS Error: fipscheck:ERROR:FIPS integrity check failed. /usr/bin/smca-fipscheck: 255
```

- If a noise source health test fails, an error message is shown on the console and the appliance halts and is not remotely accessible.

```
fipsrngdtest: Performing FIPS rngd self test...
Fatal FIPS Error: fipsrngdtest:ERROR:FIPS rngd self test failed: 1
```

If a self-test fails, see the *Reset the SMC Appliance to factory settings* topic.

Next steps

- If the self-tests succeed, continue configuring the SMC Appliance.
- If a self-test fails, restart the SMC Appliance manually. It does not restart automatically.
- If a self-test continues to fail, reset the SMC Appliance to factory settings.
To reset the SMC Appliance:
 - 1) Reboot the SMC Appliance.
 - 2) Select the **VCDROM** option from the **boot** menu.
 - 3) Start the fresh install.

Configure settings for an evaluated configuration

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

Setting	Configuration
Time Management	You can set the time manually on the SMC Appliance or you can use NTP time synchronization. By default, the Security Engine receives the time from the SMC Appliance. You can optionally also configure NTP time synchronization for the Security Engine. To use NTP time synchronization, follow the guidelines in the following topics in the <i>Configuring system communications</i> chapter in the <i>Forcepoint Network Security Platform Product Guide</i>: ■ <i>Create NTP Server elements</i> ■ <i>Enable NTP time synchronization on the SMC Appliance</i> ■ <i>Enable NTP time synchronization for Forcepoint Network Security Platform Engines</i>  Note ■ Ensure that NTP is disabled for the servers if it is not used. ■ Ensure that only secure NTP servers are selected if you are using NTP. ■ Pre-configured NTP servers cannot be used as they do not use authentication keys.
Time Management (continued)	The NTP implementation for both the SMC Appliance and the Security Engine is an NTP client only. NTP clients support communication with NTPv4 servers. By default, the SMC Appliance and Security Engine NTP clients do not update their times based on multicast or broadcast NTP packets. The NTP server must use only the SHA-1 authentication key. In 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: <pre>sudo date -s '<Day Mon DD hh:mm:ss [TZ] [YYYY]>'</pre> where <code><Day Mon DD hh:mm:ss [TZ] [YYYY]></code> 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 <i>Forcepoint Network Security Platform Product Guide</i>: ■ <i>Configuring the Log Server</i> chapter ■ <i>Using certificates to secure communications to external components</i> topic in the <i>Managing certificates for system communications</i> chapter ■ <i>Forward audit data from Management Servers to external hosts</i> topic in the <i>Reconfiguring the SMC and engines</i> 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 Network Security Platform 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 Network Security Platform cannot establish a connection with the OCSP responder, Forcepoint Network Security Platform will not accept the certificate (and thus not establish the connection). When handling certificates bearing CRL information but where Forcepoint Network Security Platform cannot establish a connection to the CRL Distribution Point location, Forcepoint Network Security Platform will not accept the certificate as valid. Forcepoint Network Security Platform 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 <i>Create Trusted Certificate Authority elements</i> topic in the <i>Managing certificates for system communications</i> chapter in the <i>Forcepoint Network Security Platform Product Guide</i>
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 <i>Create a certificate request</i> topic in the <i>Managing certificates for system communications</i> chapter in the <i>Forcepoint Network Security Platform Product Guide</i>. ■ Select either RSA or ECDSA based algorithm. For RSA available key sizes are 2048, 3072 or 4096 bits. For ECDSA available key sizes are 256 bits for P-256, 384 bits for P-384 and 521 bits for P-521. ■ 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 SMC 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:  Important - Ensure that the TLS cipher suites that is selected match the RSA and ECDSA parameters that are configured. - When using an ECDHE cipher suite, P-256, P-384, and P-521 are automatically used in the TLS key establishment. - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - TLS_ECDHE_RSA_WITH_AES_128_GCM_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_256_CBC_SHA384 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - 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 <i>Configure TLS server identity</i> topic in the <i>Managing certificates for system communications</i> chapter in the <i>Forcepoint Network Security Platform Product Guide</i>. To complete the configuration select OK in the server properties dialog box. The Log forwarding starts automatically.

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: <pre>sudo daemon-ctl restart sgMgtServer</pre> ■ Restart the Log Server on the local console. Use the command: <pre>sudo daemon-ctl restart sgLogServer</pre>
Logon Banner	To configure the Logon Banner, complete the following steps: 1) In the SMC Client, select  Settings > Global System Properties. 2) Click the Banners tab. 3) Select the Show Logon Banner checkbox and add a text to be shown on login screens in the text field below the Show Logon Banner checkbox. 4) Click the OK button.
Administrative Logins	Follow the guidelines in the <i>Administrator accounts</i> chapter in the <i>Forcepoint Network Security Platform Product Guide</i>. Use the SMC 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.  Note When the SMC Appliance Superuser option is selected, the administrator can log in to the SMC Appliance command line. Administrators with unrestricted permissions (superusers) are permitted to log in to the SMC Appliance command line only if there are no other administrators with SMC Appliance Superuser permissions active.

Setting	Configuration
Administrative Logins (continued)	To specify the timeout to terminate an inactive local administrative session, enter: <pre>TMOUT=<TIMEOUT>;echo "export TMOUT=\$TMOUT" >> ~/.bashrc;logger -s -p local3.info "changed console timeout to \$TMOUT"</pre> where <code><TIMEOUT></code> is the timeout in seconds. To enable temporarily locking administrator accounts after a certain amount of failed logon attempts: 1) In the SMC Client, select  Settings > 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 SMC Client, select  Settings > 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 SMC Client Window After the User Session is Idle for and select Close the SMC 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 SMC Client and locking administrator accounts, see the <i>Enable and define password policy settings</i> topic in the <i>Administrator accounts</i> chapter in the <i>Forcepoint Network Security Platform Product Guide</i>
Administrative Logins (continued)	To manually log out of the local console account, enter: <pre>logout</pre> To log out of the SMC Client, select  Admin User Menu > Exit.

Setting	Configuration
Password Guidelines	Follow the guidelines in the <i>Enable and define password policy settings</i> topic in the <i>Administrator accounts</i> chapter in the <i>Forcepoint Network Security Platform Product Guide</i>. 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 Network Security Platform 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.  Note Use strong passwords that are at least 15 characters long and contain a combination of numbers, letters, and special characters. Do not base passwords on personal information such as names, birthdays, ID numbers, phone numbers, street names, registration plate numbers, or names of relatives.
Engine Policy	Use the Firewall Template Policy as the basis for creating a customized Engine Template Policy and security policies that are compliant with Common Criteria. For more information, see the topics in this document about creating a customized Engine Template Policy and creating a Engine Policy. See also the <i>Creating and managing policy elements</i> chapter and the <i>Access rules</i> chapter in the <i>Forcepoint Network Security Platform Product Guide</i>.
Web Access	If you use the Web Access feature to use the SMC Client in a web browser, do the following: ■ In the Management Server Properties dialog-box, click the Web Access tab. ■ Select the Enable checkbox. ■ Select the Use Internal Certificate checkbox to use the same certificate that is issued for the Management Server. ■ Select only the following algorithms for the TLS Cryptography Suite Set element: ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ■ Click OK. For more details on Web Access configuration, refer to the <i>Using the SMC Client in a web browser</i> section in the <i>Forcepoint Network Security Platform Product Guide</i>.

Additionally, when SMC acts as the TLS client for log or audit data forwarding, the list of supported algorithms in the TLS signature_algorithms extension is fixed to:

- rsa_pkcs1_with_sha256(0x0401)
- rsa_pkcs1with sha384(0x0501)
- rsa_pkcs1_with_sha512(0x0601)
- ecdsa_secp256r1_with_sha256(0x0403)
- ecdsa_secp384r1_with_sha384(0x0503)

- `ecdsa_secp521r1_with_sha512(0x0603)`
- `rsa_pss_rsae_with_sha256(0x0804)`
- `rsa_pss_rsae_with_sha384(0x0805)`
- `rsa_pss_rsae_with_sha512(0x0806)`
- `rsa_pss_pss_with_sha256(0x0809)`
- `rsa_pss_pss_with_sha384(0x080a)`
- `rsa_pss_pss_with_sha512(0x080b)`

Deleting log and audit data

The Security Engine stores log data temporarily until the data is sent to the Log Server. The Log Server is responsible for sending log data to the configured external audit server.

The Management Server and Log Server store audit and log data locally, then send the data to an external audit server. Locally stored audit and log data cannot be modified. Locally-stored data is not deleted automatically. Administrator can manage locally stored log and audit retention period by configuring log deletion tasks as instructed in the *Managing log data* chapter in the *Forcepoint Network Security Platform Product Guide*. 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 Security 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 **Network Elements**.
- 2) Browse to **Servers**.
- 3) Right-click the **Management Server**, then select **Properties**.
- 4) In the **Audit Storage Full** field on the **General** tab, select **Stop Management Server**.
- 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 **Network Elements**.
- 2) Browse to **Servers**.
- 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 Security Engine

The Security 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 Security 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 Security Engine as explained in section, *Create an element for the Security Engine*.

Steps

- 1) Set the **Log Spooling Policy** option to **Stop Traffic**.
When the Log Spooling Policy option is set to **Stop Traffic**, the Security 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 Security 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 Network Security Platform Product Guide*. For more details about the product and how to configure features, click **Help** or press **F1**.

Steps

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

Create an element for the Security Engine

Use the SMC Client to create the Security Engine element.

These steps are the high-level tasks. For more information, see the *Creating and modifying Security Engines* chapter in the *Forcepoint Network Security Platform Product Guide*.

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

- 1) In the SMC Client, create an Security Engine, then define the properties in the Engine Editor. Follow the normal process to define the properties of an Security 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**.
- 2) Save the initial configuration.



Note

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

Limit half-open TCP connections

Forcepoint Security Engine 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 Security Engine as a whole or for a specific rule).

When the Security Engine detects that the threshold has been exceeded, the Security Engine denies additional SYN packets. The Security 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 Security Engine 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 Security Engine, but can be overridden for some traffic in the Access rule options in a Engine 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 Engine Template Policy

For a Common Criteria installation, add specific Access rules to a customized Engine Template Policy, 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 Network Security Platform 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 Engine Template Policy for editing, then save it as Engine cPP Template.

2) Create the following Network elements:

- For IPv4, 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
Link-Local IPv4 Unicast Addresses	ANY	ANY	Discard
ANY	Link-Local IPv4 Unicast Addresses	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 addresses	ANY	ANY	Discard
ANY	IPv6 RFC 3513 reserved addresses	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 below rules before the IPv6 Insert Point. "IPv6 Solicited-Node Multicast" is defined as `FF02::1:FF00:0/104`.



Note

You must define the IPv6 Solicited-Node Multicast network before you add the rules.

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
RFC 3513 Global Unicast Addresses, Link-Local IPv6 Unicast Addresses	Link-Local IPv6 Unicast Addresses	IPv6 Neighbor Advertisement	Allow

Create a Engine Policy

After creating the customized Engine Template Policy, create a Engine 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 Network Security Platform 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 Network Security Platform Product Guide*.

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

- 1) Create a Engine Policy that uses the Engine 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 Security 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 SMC Client to create the Security Engine element. This is described in detail in section *Create an element for the Security 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, *Define a VPN site for internal private networks*.
- 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 Security 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 Security Engine.

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

- 1) Right-click the Engine, then select **Edit Single Engine** or **Edit Cluster Engine**.
 - 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 Engine's default routing table.
 - If loopback IP addresses are defined for the Security 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 Engine.
- 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 Security 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 Engine element, then select **Edit Single Engine**.
- 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 Engine (for interfaces that are not disabled).
- 4) Click  **Save**.

Define a VPN site for internal private networks

You must define site elements for all Security 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 Security 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 Security 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 Engine, then select **Edit Single Engine** 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 Engine, then select **Edit Single Engine**.
- 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 Engine 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 (CA).



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.

**Important**

Below are the requirements for a root certificate:

- The following types of authentication key are only accepted:
 - For Common Criteria evaluated configuration:
 - RSA-2048
 - RSA-2072
 - RSA-4096
 - ECDSA P-256
 - ECDSA P-384
 - ECDSA P-521
 - For Commercial Solutions for Classified configuration:
 - RSA-3072
 - RSA-4096
 - ECDSA P-384
- The digest algorithm must be one of the following:
 - For Common Criteria evaluated configuration:
 - SHA-1
 - SHA-256
 - SHA-384
 - SHA-512
 - For Commercial Solutions for Classified configuration:
 - SHA-384
 - SHA-512
- All the certificates in the chain that is signed by the root certificate must have either a Certificate Revocation List (CRL) distribution point, or an Online Certificate Status Protocol (OCSP) server URL, or both. Additionally, OCSP or CRL checking must be enabled in the root CA settings.

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 Security Engine 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 Network Security Platform supports OCSP and CRL revocations for X.509v3 certificate validation during negotiation of IPsec VPN.

Forcepoint Network Security Platform 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 Network Security Platform 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 Network Security Platform 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 Network Security Platform cannot determine revocation status using OCSP, revocation status is checked using a CRL.
- When either OCSP or CRLs are enabled and Forcepoint Network Security Platform cannot determine the revocation status, Forcepoint Network Security Platform 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  **Secure SD-WAN Configuration**.
- 2) Browse to **Other Elements > VPN 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 Engine Policy is based on the Engine Template, both LDAP (port 389) and HTTP (port 80) connections from the Engine are allowed. If your Engine or server configuration differs from these standard definitions, edit the Engine 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 **Secure SD-WAN Configuration**.
- 2) Select **VPN Gateways**.
The gateways are displayed.
- 3) Right-click the VPN Gateway element and select **More actions > 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. It can be either RSA or ECDSA.

- 8) Select the **Signature Algorithm** that the certificate authority uses to sign the certificate:
 - For Common Criteria evaluated configuration and RSA, select RSA / SHA-1, RSA / SHA-256, RSA / SHA-384, or RSA / SHA-512.
 - For Common Criteria evaluated configuration and ECDSA, select ECDSA / SHA256, ECDSA / SHA384 or ECDSA / SHA512.
 - For Commercial Solutions for Classified configuration and RSA, select RSA / SHA-384 or RSA / SHA-512.
 - For Commercial Solutions for Classified configuration and ECDSA, select ECDSA / SHA384 or ECDSA / SHA512.
- 9) Select the Key Length:
 - For Common Criteria evaluated configuration:
 - **RSA**: 2048, 3072, or 4096 are allowed
 - **ECDSA**: 256, 384, or 521 are allowed
 - For Commercial Solutions for Classified configuration:
 - **RSA**: 3072 or 4096 are allowed
 - **ECDSA**: Only 384 is allowed
- 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 particular, 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 VPN configuration 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  **Secure SD-WAN Configuration**.
- 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.

Option	Definition
Cipher Algorithms	Select the encryption method: ■ For Common Criteria evaluated configuration: ■ AES-GCM-256: Advanced Encryption Standard (AES) and Galois/Counter Mode (GCM) encryption algorithm with a 256-bit key size. Recommended for high-speed networks. ■ AES-CBC-256: Advanced Encryption Standard (AES) and Cipher Blocking Chaining (CBC) encryption algorithm with a 256-bit key size. ■ AES-CBC-128: Advanced Encryption Standard (AES) and Cipher Blocking Chaining (CBC) encryption algorithm with a 128-bit key size. Note When AES-CBC-128 is selected, the Security Engine also supports AES-CBC-192 when acting as the responder in the negotiation. ■ For Commercial Solutions for Classified configuration: ■ AES-GCM-256: Advanced Encryption Standard (AES) and Galois/Counter Mode (GCM) encryption algorithm with a 256-bit key size. Recommended for high-speed networks. ■ AES-CBC-256: Advanced Encryption Standard (AES) and Cipher Blocking Chaining (CBC) encryption algorithm with a 256-bit key size.
Integrity / Pseudorandom Function Algorithms	Used for integrity checking and key derivation. Select SHA-2 with 256, 384 or 512 bit minimum length to enable SHA-256, SHA-384, or SHA-512 for IKE. ■ SHA-2 — The SHA-2 set of hash function includes SHA-256, SHA-384, and SHA-512.
Key Exchange Methods	Select one or more groups for key exchange. ■ For Common Criteria evaluated configuration: ■ 21 (ECP 521 bits) — Diffie-Hellman key exchange with 521-bit elliptic curve. ■ 20 (ECP 384 bits) — Diffie-Hellman key exchange with 384-bit elliptic curve. ■ 19 (ECP 256 bits) — Diffie-Hellman key exchange with 256-bit elliptic curve. ■ 18 (8192 bits) — Diffie-Hellman key exchange with a 8192 bit modulus. ■ 17 (6144 bits) — Diffie-Hellman key exchange with a 6144 bit modulus. ■ 16 (4096 bits) — Diffie-Hellman key exchange with a 4096-bit modulus. ■ 15 (3072 bits) — Diffie-Hellman key exchange with a 3072-bit modulus. ■ 14 (2048 bits) — Diffie-Hellman key exchange with a 2048-bit modulus. ■ For Commercial Solutions for Classified configuration: ■ 20 (ECP 384 bits) — Diffie-Hellman key exchange with 384-bit elliptic curve. ■ 19 (ECP 256 bits) — Diffie-Hellman key exchange with 256-bit elliptic curve. ■ 16 (4096 bits) — Diffie-Hellman key exchange with a 4096-bit modulus. ■ 15 (3072 bits) — Diffie-Hellman key exchange with a 3072-bit modulus.

Option	Definition
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. ■ For Common Criteria evaluated configuration: ■ ECDSA Signatures — Requires that each Gateway has a valid certificate. ■ Pre-Shared Key — Requires that you periodically change the pre-shared keys for each tunnel in the VPN elements to be secure. ■ RSA Signatures — Requires that each Gateway has a valid certificate. ■ For Commercial Solutions for Classified configuration: ■ 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 tunnels. Mobile VPNs have separate settings on the IPsec Client tab.
IKEv2 PPK	Select one of the following options for Post-quantum Pre-Shared Key (PPK): ■ Not in use — PPK is not enabled. ■ Enabled — PPK is enabled to use with IKEv2 protocol for the tunnel but is not mandatory. For example, if we want to establish a tunnel between Gateway A and Gateway B. Gateway A has PPK enabled and configured but Gateway B does not support PPK feature or PPK is not configured. Then the tunnel can still be established without the PPK. ■ Mandatory — PPK is enabled and is mandatory to use with IKEv2 protocol for the tunnel to be established. For example, if we want to establish a tunnel between Gateway A and Gateway B. Gateway A has PPK enabled and configured but Gateway B does not support PPK feature or PPK is not configured. Then the tunnel cannot be established without the PPK configured on both gateways. Note ■ For Commercial Solutions for Classified configuration only the Mandatory option is allowed. ■ A single PPK element is defined for the gateway-to-gateway tunnel, and the element is auto-generated if both are internal gateways.
SA Lifetime in Minutes	The time limit after which IKE SA negotiations are done again in a continuously used tunnel. 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 Security Engine keeps the IPsec tunnels established even when no traffic is sent through the 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 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	Select the tunnel encryption method. ■ For Common Criteria evaluated configuration: ■ AES-GCM-256: Advanced Encryption Standard (AES) and Galois/Counter Mode (GCM) encryption algorithm with a 256-bit key size. Recommended for high-speed networks. ■ AES-GCM-128: Advanced Encryption Standard (AES) and Galois/Counter Mode (GCM) encryption algorithm with a 128-bit key size. Recommended for high-speed networks.  Note When AES-GCM-128 is selected, the Security Engine also supports AES-GCM-192 when acting as the responder in the negotiation. ■ AES-256: Advanced Encryption Standard (AES) and Cipher Blocking Chaining (CBC) encryption algorithm with a 256-bit key size. ■ AES-128: Advanced Encryption Standard (AES) and Cipher Blocking Chaining (CBC) encryption algorithm with a 128-bit key size.  Note When AES-128 is selected, the Security Engine also supports AES-192 when acting as the responder in the negotiation. ■ For Commercial Solutions for Classified configuration: ■ AES-GCM-256: Advanced Encryption Standard (AES) and Galois/Counter Mode (GCM) encryption algorithm with a 256-bit key size. Recommended for high-speed networks. ■ AES-256: Advanced Encryption Standard (AES) and Cipher Blocking Chaining (CBC) encryption algorithm with a 256-bit key size.

Option	Definition
Integrity Algorithms	Select the cryptographic method: ■ For Common Criteria evaluated configuration, SHA-1 or SHA-2 with a minimum length of 256 bit is supported. ■ For Commercial Solutions for Classified configuration, SHA-2 with a minimum length of 384 bit is supported.
Compression Algorithm	Options for compressing the data in the tunnel to reduce the bandwidth use on congested links. ■ None — (Recommended for most environments) Sends the data without compressing it. Provides better performance when bandwidth congestion for tunneled traffic is not a constant issue or if there is significant processor load. ■ Deflate — Compresses the data. This compression requires processing and memory resources, which increases latency. Latency might also increase for non-tunneled traffic. Do not select this option if the resource utilization is high. Gateways at both ends of each tunnel involved must support the option.
IPsec Tunnel Lifetime (Optional)	Limits after which IPsec SA negotiations are done again in a continuously used tunnel. 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.
Use PFS (Optional)	Enables the Perfect Forward Secrecy (PFS) feature.  Note When the PFS feature is enabled. By default, the Same as in IKE option is selected for the PFS Key Exchange Method.

Option	Definition
PFS Key Exchange Method	Select the default value Same as in IKE.  Note ■ By default, the Same as in IKE option is selected. This means the option enforces selection of the same Diffie-Hellman group for PFS that was selected for the IKE SA key exchange. ■ If an option other than the Same as in IKE option is selected, an error message that states "<i>Explicit PFS Key Exchange Method selection will be deprecated in a future version. Change selection to 'Same as in IKE' in Profile configuration.</i>" is displayed during the policy upload. 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.
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 tunnel 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 IPsec client settings is used in a route-based tunnel, the IPsec Client settings are ignored.

Option	Definition
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.
Allow Hybrid / EAP Authentication (Optional) (Forcepoint VPN Client only)	Allows users of the Forcepoint VPN Client to authenticate by filling in a user name and password or a similar authentication scheme provided by an external authentication server. The gateway still authenticates itself to the VPN clients using a certificate.
Allow CN Authentication (Optional) (Certificate authentication only)	Allows using the common name (CN) of the certificates for authentication. The CN is checked against a value entered in User elements.
Allow Pre-Shared Key Authentication with IKEv1 (Optional)	Select this option if you have third-party VPN clients that use a pre-shared key for authenticating the VPN clients and the gateway. The pre-shared key is defined in the properties of User elements that have Pre-Shared Key Method as an authentication method. The Forcepoint VPN Client does not support this method.  CAUTION The pre-shared key option requires aggressive mode IKE negotiations in the mobile VPN. In aggressive mode, user information is not protected, so we recommend that you take precautions, such as not using the same user name for the users as they have when they access other services in your internal network.

Option	Definition
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 tunnel. This setting reduces the overhead when there are many hosts making connections through the tunnel. ■ 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 tunnel. 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.  Note SA per Host is valid only for 3rd Party IPsec VPN Clients.

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.

Create Post-quantum Pre-shared Key element

A Post-quantum Pre-shared Key (PPK) element can be used along with the IKEv2 protocol to prevent threats from quantum computers. A PPK consists of a Key ID and a Pre-shared secret.

Steps

- 1) Select  **Secure SD-WAN Configuration**.
- 2) Select **Other Elements > Post-quantum Preshared Keys**.
- 3) Right-click **Post-quantum Preshared Keys**, then select **New Post-quantum Preshared Key**.
- 4) Configure the settings.
- 5) Click **OK**.

Post-quantum Preshared Key Properties dialog box

Use this dialog box to create a new PPK element.

Option	Definition
Name (Optional)	Enter a name for the PPK element for easy identification.  Note If the name field is left empty, then the primary PPK ID is used as the name of the element.
Primary PPK section	
ID	Enter the primary PPK ID.  Note The PPK ID is a string that can be between 1 and 1024 characters long.
Secret	Enter the pre-shared secret that is associated with the primary PPK ID.  Note If you want to change the primary pre-shared secret on both gateways, first define the new secret in the Secondary PPK section and then use the Swap button to swap between the primary and secondary secret. For more details, refer to the <i>Update the Post-quantum Pre-shared key</i> topic in the <i>Forcepoint Network Security Platform Product Guide</i>.  Note - The Secret can be one of the following: - An ASCII string. - A hex-encoded string if it has a 0x prefix in its value. - A Base64-encoded string if it has a 0s prefix in its value. - The secret must have minimum of 256 bits of entropy. For example, 32 bytes of cryptographically secure random data encoded as hex or base64.
Hide	When selected, the primary pre-shared secret is hidden.
Swap	Click the Swap button to swap between the primary and secondary PPK ID and Secret pairs.
Secondary PPK section	

Option	Definition
ID (Optional)	Enter the secondary PPK ID.  Note The PPK ID is a string that can be between 1 and 1024 characters long.
Secret (Optional)	Enter the pre-shared secret that is associated with the secondary PPK ID.  Note - The Secret can be one of the following: - An ASCII string. - A hex-encoded string if it has a 0x prefix in its value. - A Base64-encoded string if it has a 0s prefix in its value. - The secret must have minimum of 256 bits of entropy. For example, 32 bytes of cryptographically secure random data encoded as hex or base64.
Hide	When selected, the secondary pre-shared secret is hidden.
Comment (Optional)	Enter a comment for the PPK element for easy identification.

Setup external VPN Gateway element

External VPN Gateway elements represent third-party VPN devices or Forcepoint Network Security Platform devices managed by a different Management Server. To use third-party VPN devices or Forcepoint Network Security Platform 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 Network Security Platform devices managed by a different Management Server. To use third-party VPN devices or Forcepoint Network Security Platform 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 ⓘ **Secure SD-WAN Configuration**.

- 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 Engine.

- 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 Security 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 Security 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 Security 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  **Secure SD-WAN Configuration**.
- 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 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 Engine.

Activate the internal DHCP server on a Engine interface

You can use the internal DHCP server in Engine 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 Security Engine, then select **Edit Single Engine**.
- 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 Security 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  **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 Engine, then select **Edit Single Engine**.
- 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 Engine 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 Engine 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 Engine 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 **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 Security Engines

The internal user database on the Management Server is replicated automatically to 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 Engine, Engine Cluster, or Master Security Engine and select or deselect **Options > User DB Replication**.

Reset a Engine's local user database

You can replace the Engine'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 Engine 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 Engine or individual nodes of a Engine 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 **Secure SD-WAN Configuration**.
- 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  **Engine Configuration**.
- 2) Browse to **Engine > Policies > Engine Policies**.
- 3) Right-click the Engine policy that is used by the Security Engines involved in the VPN, then select **Edit Engine 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  **Engine Configuration**.
- 2) Browse to **Engine > Policies > Engine Policies**.
- 3) Right-click the Engine policy that is used by the Security Engines involved in the VPN, then select **Edit Engine 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  **Engine Configuration**.
- 2) Browse to **Engine > Policies > Engine Policies**.
- 3) Right-click the Engine policy that is used by the Security Engines involved in the VPN, then select **Edit Engine 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.	Right-click the Action cell, and then select the Edit option. 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 Engine template policy

Modify the Engine template policy 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.
- You can use Source match to block access based on IP address.

Steps

- 1) Select  **Engine Configuration**.
- 2) Browse to **Other Elements**.
- 3) Right-click **Rule Validity Time**, then select **New Rule Validity Time**.
- 4) 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**.
- 5) Click **OK**.
- 6) Open the Engine cPP Template for editing.
- 7) 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
```

- 8) Save the template policy.
- 9) 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 Engine 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 template policy.
- 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 Engine 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 Engine 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 Security Engine

The target of evaluation uses a registration process to join Security Engines to the SMC using a registration channel. The administrator enables the Security 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 Security

Engine console to initiate the registration process. The Security 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 Security Engine is installed in FIPS mode using the 256-bit security setting according to Install the Security Engine in FIPS mode.
- Verify that the Virtual SMC is connected to the management network using its management network interface.
- Verify that the joining Engine is connected to the management network using its management network interface.

The SMC and Security 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. Security 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 Security Engine using an SMC generated one-time password that the administrator inputs into the Engine.

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

In the 256-bit mode ECDSA P-384 with SHA-384 digital signatures is used in all certificates for the communication between SMC and Security 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.

Recovering from a failed registration

If the registration process is interrupted or fails due to a connectivity issue, restart the process from the **Save the initial configuration in the SMC Client** step once connectivity has been restored.

Recovering from a failed management connection after successful registration between Security Engine and SMC

If management connectivity between the SMC and Security Engine fails after registration has been completed, follow these general steps to recover:

- Check network connectivity between the Security Engine, SMC and CA infrastructure in use.
- Check the SMC logs for error messages.
- Check that none of the certificates involved has expired. To renew certificate of each component, see corresponding section in this guide:
 - Renew a certificate for the Management Server.
 - Renew a certificate for the Log Server.
 - Renew a certificate for the Security Engine.
- Contact Forcepoint support as a last resort.

Save the initial configuration in the SMC Client

You must save the initial configuration for the Security Engine.

Steps

- 1) Select  **Engine Configuration**.
- 2) Right-click the Security Engine, then select **Configuration > Save Initial Configuration**.
- 3) Next to the **Initial Security Policy** field, click **Select**, then select the Engine Policy that you created. The policy is automatically installed on the Security 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 Security Engine.
- 5) Click **OK**.

Install the Security Engine in FIPS mode

To comply with Common Criteria evaluation standards, you must enable FIPS-compatible mode and enable 256-bit encryption as the security strength when you configure the Security Engine using the Security Engine Configuration Wizard.

The Security Engine uses TLS 1.2 and the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suite for management connections with the SMC.



Note

If the Security Engine is installed as a Virtual Machine in ESXi, the same ESXi entropy configuration caveats apply as in the *Enable FIPS mode on the SMC Appliance* topic.

These steps are the high-level tasks. For complete installation instructions, see the *Forcepoint Network Security Platform Installation Guide*. Before upgrading, read the *Forcepoint Network Security Platform Release Notes* for the version you are upgrading to.



Note

Security Engine appliances come with Security Engine software pre-installed. Before setting the Security Engine to use FIPS mode, upgrade the Security Engine software to the version that you want to use.

Steps

- 1) Download the Security Engine software from <https://support.forcepoint.com/s/download>, then validate the checksums.



Note

Save the Security Engine upgrade .zip file to the root directory of the USB drive or DVD media.

For information about obtaining the installation files, see the *Forcepoint Network Security Platform Installation Guide*.

- 2) Upgrade the Security Engine software to the version that you want to use.
 - a) In the Security Engine Configuration Wizard, select **Upgrade**.
 - b) In the **Select Source Media** dialog box, select the appropriate media type, then click **OK**.
The software update signature is verified.
 - c) Click **OK**.
The upgrade starts.
 - d) Select **Set kernel in FIPS mode after reboot**.
 - e) Click **OK**.
Security Engine appliance restarts and displays the upgraded version.
- 3) Configure the Security Engine with the Security Engine Configuration Wizard.
Follow the normal process to define the Security Engine properties, with these exceptions:
 - Select **Restricted FIPS-Compatible Operating Mode**.
This option enables the FIPS 140-3 cryptographic module.
 - Ensure that the **256-bit security strength** is selected in the Management Server configuration settings.

**Note**

This option is selected by default.

- 4) To verify FIPS-Approved mode of operation, verify that the following messages are shown on the console when the Security Engine appliance restarts:

```
FIPS: rootfs integrity check OK
```

This message confirms that the module's integrity test has been executed successfully. The integrity test verifies an ECDSA P-521 signature with SHA-512 over the root file system. If the integrity test fails, an error message is displayed and the module restarts.

```
FIPS power-up tests succeeded
```

This message confirms that the FIPS power-up self-tests have been executed successfully. If the power-up tests fail, a power-up test error message is shown and the module restarts.

If the connection with the Management Server is not established successfully, verify the following:

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

Verify the Security Engine self-tests

The Security Engine contains the Forcepoint Network Security Platform FIPS Library, Forcepoint Network Security Platform FIPS Cryptographic Module, and Forcepoint Network Security Platform Cryptographic Kernel Module. The modules run several self-tests when the Forcepoint Network Security Platform appliance starts.

The modules perform these tests:

- Cryptographic Algorithm Self-Tests (CAST) implemented as Known Answer Tests (KAT)
- Forcepoint Network Security Platform FIPS Library self-tests
- Forcepoint Network Security Platform FIPS Cryptographic Module self-tests
- Forcepoint Network Security Platform Cryptographic Kernel Module self-tests

Forcepoint Network Security Platform FIPS Library self-tests

Algorithm	Type	Test Method
HMAC-SHA2- 256	SW/FW Integrity	Message Authentication
AES-ECB	CAST	KAT
AES-GCM	CAST	KAT
Counter DRBG	CAST	KAT
DSA SigGen (FIPS186-4)	CAST	KAT
DSA SigVer (FIPS186-4)	CAST	KAT
ECDSA SigGen (FIPS186-4)	CAST	KAT
ECDSA SigVer (FIPS186-4)	CAST	KAT
Hash DRBG	CAST	KAT
HMAC DRBG	CAST	KAT
HMAC-SHA2-256	CAST	KAT
KASECC-SSC Sp800-56Ar3	CAST	KAT
KAS-FFCSCC Sp800-56Ar3	CAST	KAT
KAS-IFCSCC	CAST	KAT
KDF SP800-108	CAST	KAT
KDA OneStep SP800-56Cr2	CAST	KAT
KDA TwoStep SP800-56Cr2	CAST	KAT
KTS-IFC	CAST	KAT
KTS-IFC	CAST	KAT
PBKDF	CAST	KAT
RSA SigGen (FIPS186-4)	CAST	KAT
RSA SigVer (FIPS186-4)	CAST	KAT
SHA-1	CAST	KAT
SHA2-512	CAST	KAT
SHA3-256	CAST	KAT
KDF ANS 9.42	CAST	KAT
KDF ANS 9.63	CAST	KAT
KDF SSH	CAST	KAT
TLS v1.2 KDF RFC7627	CAST	KAT
TLS v1.3 KDF	CAST	KAT

Algorithm	Type	Test Method
RSA KeyGen (FIPS186-4)	Pair-Wise Consistency Test	PCT
ECDSA KeyGen (FIPS186-4)	Pair-Wise Consistency Test	PCT
DSA KeyGen (FIPS186-4)	Pair-Wise Consistency Test	PCT
ECDSA SigGen (FIPS186-4)	CAST	KAT
ECDSA SigVer (FIPS186-4)	CAST	KAT
HMAC-SHA2-256	CAST	KAT
AES-ECB	CAST	KAT
AES-GCM	CAST	KAT
AES-GCM	CAST	KAT
Counter DRBG	CAST	KAT
DSA SigGen (FIPS186-4)	CAST	KAT
DSA SigVer (FIPS186-4)	CAST	KAT
ECDSA SigGen (FIPS186-4)	CAST	KAT
ECDSA SigVer (FIPS186-4)	CAST	KAT
Hash DRBG	CAST	KAT
HMAC DRBG	CAST	KAT
HMAC-SHA2-256	CAST	KAT
KAS-ECC-SSC Sp800-56Ar3	CAST	KAT
KAS-FFC-SSC Sp800-56Ar3	CAST	KAT
KAS-IFC-SSC	CAST	KAT
KDF SP800-108	CAST	KAT
KDA OneStep SP800-56Cr2	CAST	KAT
KDA TwoStep SP800-56Cr2	CAST	KAT
KTS-IFC	CAST	KAT
KTS-IFC	CAST	KAT
PBKDF	CAST	KAT
RSA SigGen (FIPS186-4)	CAST	KAT
RSA SigVer (FIPS186-4)	CAST	KAT
SHA-1	CAST	KAT
SHA2-512	CAST	KAT
SHA3-256	CAST	KAT
KDF ANS 9.42	CAST	KAT
KDF ANS 9.63	CAST	KAT
KDF SSH	CAST	KAT
TLS v1.2 KDF RFC7627	CAST	KAT

Algorithm	Type	Test Method
TLS v1.3 KDF	CAST	KAT
RSA KeyGen (FIPS186-4)	Pair-Wise Consistency Test	PCT
ECDSA KeyGen (FIPS186-4)	Pair-Wise Consistency Test	PCT
DSA KeyGen (FIPS186-4)	Pair-Wise Consistency Test	PCT
ECDSA SigGen (FIPS186-4)	CAST	KAT
ECDSA SigVer (FIPS186-4)	CAST	KAT

Forcepoint Network Security Platform FIPS Cryptographic Module self-tests

Algorithm	Type	Test Method
ECDSA signature verify with NIST P-224 and SHA2-224	Software Integrity	
SHA-1	CAST	KAT
SHA2-512	CAST	KAT
SHA3-224	CAST	KAT
HMAC-SHA2-256	CAST	KAT
AES-CBC encryption (128-bit key)	CAST	KAT
AES-CBC decryption (128-bit key)	CAST	KAT
AES-CCM encryption (128-bit key)	CAST	KAT
AES-CCM decryption (128-bit key)	CAST	KAT
AES-GCM encryption (128-bit key)	CAST	KAT
AES-GCM decryption (128-bit key)	CAST	KAT
AES-XTS encryption (128-bit key strength)	CAST	KAT
AES-XTS decryption (128-bit key strength)	CAST	KAT
AES-CMAC (192-bit key)	CAST	KAT
TDES-CBC encryption (192-bit key)	CAST	KAT
TDES-CBC decryption (192-bit key)	CAST	KAT
Counter DRBG AES-256 (instantiate, generate and reseed; includes AES-ECB mode encryption)	CAST	KAT
RSA SigGen 2048-bit with SHA2-256	CAST	KAT

Algorithm	Type	Test Method
RSA SigVer 2048-bit with SHA2-256	CAST	KAT
DSA SigGen (P=2048/N=256 with SHA2-224)	CAST	KAT
DSA SigVer (P=1024/N=160 with SHA2-224)	CAST	KAT
ECDSA SigGen (NIST P-224 with SHA2-224)	CAST	KAT
ECDSA SigVer (NIST P-224 with SHA2-224)	CAST	KAT
KTS-IFC Key Encapsulation 2048-bit (RSA-OAEP)	CAST	KAT
KTS-IFC Key Un-encapsulation 2048-bit (RSA-OAEP)	CAST	KAT
KAS-FFC-SSC (P=2048/N=224)	CAST	KAT
KAS-ECC-SSC (NIST P-224)	CAST	KAT
KDF SP800-108 (Counter Mode)	CAST	KAT
KDA HKDF (includes KDF SP800-108 Feedback Mode)	CAST	KAT
KDF SP800-108 (Double Pipeline Mode)	CAST	KAT
KDF IKEv1	CAST	KAT
KDF IKEv2	CAST	KAT
TLS v1.2 KDF RFC7627	CAST	KAT
SP 800-90A-r1, (Instantiate/Generate) health tests for Counter DRBG AES-256	CAST	KAT
SP 800-90A-r1, (Reseed) health test Counter DRBG AES-256	CAST	KAT
SP 800-90B, start-up and continuous health tests (RCT and APT) for JitterEntropy ENT (NP)	CAST	Fault Detection Tests

Forcepoint Network Security Platform Cryptographic Kernel Module self-tests

Algorithm	Type	Test Method
HMAC-SHA2-256	Software Integrity	Message Authentication
AES encryption (AES-CBC, AES-CFB128, AES-ECB, AES-OFB 128, 192, 256)	CAST	KAT

Algorithm	Type	Test Method
AES decryption (AES-CBC, AES-CFB128, AES-ECB, AES-OFB 128, 192, 256)	CAST	KAT
AES-GCM 128 authenticated encryption	CAST	KAT
AES-GCM 128 authenticated decryption	CAST	KAT
SHA (SHA-1, SHA2-256, SHA2- 512)	CAST	KAT
HMAC (HMAC-SHA-1, HMACSHA2-256, HMAC-SHA2- 512)	CAST	KAT

Check the self-test results in the console.

- If a cryptographic self-test or a noise source health test fails, an error message is shown on the console and the appliance is restarted automatically. Noise source health tests are automatically executed as part of the self-tests when Forcepoint Network Security Platform FIPS Library and Forcepoint Network Security Platform FIPS Cryptographic Module are loaded.

```
FIPS: OpenSSL self-tests FAILED, rebooting...
Cryptographic Kernel Module self tests failed
FIPS: Cryptographic module self-tests FAILED, rebooting...
```

```
FIPS: rootfs integrity check FAILED, rebooting...
```

Next steps

- If the self-tests succeed, continue configuring the Security Engine.
- If the problem persists, reset the Security Engine to factory settings. To reset the Security Engine, do the following:
 - 1) Power off the Security Engine.
 - 2) Power on the Security Engine, and select the **System restore options** option from the local console **boot** menu.
 - 3) Follow the instructions to reset the Security Engine.

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

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

Verify the SMC version

You can verify the SMC version in the SMC Client.

Steps

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

Verify the Security Engine version

You can verify the Security Engine version in the SMC Client.

Steps

- 1) Select **Dashboards > Engines Dashboard**.
- 2) Expand the nodes of the engine for which you want to verify the version.
- 3) Right-click the Security Engine and select **Properties**.
On the **General** tab of the **Info** pane, the Security 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 Security Engine

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

Disable in the SMC by deleting the Security Engine element

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

Steps

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

Disable by resetting the Security Engine in the SMC Client

You can reset the Security Engine to factory settings from the SMC Client.

Steps

- 1) Select  **Engine Configuration**.
- 2) Right-click the Security 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 Security Engine from the console

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



Note

- If a cryptographic self-test or the file system integrity check fails, you must reset the appliance to factory settings.
- If the appliance is otherwise functioning correctly, but you want to destroy all cryptographic keys on the Security Engine appliance, you can also reset the appliance to factory settings from the SMC Client. For more information, see the *Forcepoint Network Security Platform Product Guide*.

Steps

- 1) Restart the Forcepoint Network Security Platform appliance, then select **System restore options** from the boot menu.
- 2) Select **Advanced data removal options**.
- 3) Select the number of overwrite passes.
A larger number of overwrites is more secure, but it might take a considerable amount of time depending on the appliance storage capacity.
 - For one pass, select **1 pass overwrite**.
 - For multiple passes, select **Custom**, then enter the number of overwrite passes.
- 4) Install the Security Engine 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 Security Engines* chapter in the *Forcepoint Network Security Platform Product Guide*. Some of the more common McAfee ESM fields are described in the following table.

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

Field	Description
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 "Engine" for Management Server, Log Server, and Security 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	<pre>Timestamp="2025-03-17 16:45:35", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="2665877378764374017", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.start", Result="Success", ObjectName="Audit function started"</pre> <pre>Timestamp="2025-03-17 16:47:09", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", SenderType="Log Server", EventId="2666279465012690945", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.start", Result="Success", ObjectName="Audit function started"</pre>

FAU_GEN.1.1 a)	
Shutdown of SMC Appliance	<pre>Timestamp="2025-03-17 16:48:58", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="2665770623057264758", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.stop", Result="Success", ObjectName="Audit function shutdown"</pre> <pre>Timestamp="2025-03-17 16:51:14", NodeId="192.0.2.2", CompId="LogServer 192.0.2.2", SenderType="Log Server", EventId="2666399363319726188", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="audit.stop", Result="Success", ObjectName="Audit function shutdown"</pre>
Startup of Security Engine	<pre>Timestamp="2025-03-17 16:44:28", LogId="1803", NodeId="192.0.2.4", Facility="System Utilities", Type="Notification", CompId="ngfw node 1", InfoMsg="Auditing log start", ReceptionTime="2025-03-17 16:47:21", SenderType="Firewall", SituationId="78022", Situation="System_Engine-Log-Auditing-State", EventId="7307441706553575179"</pre>
Shutdown of Security Engine	<pre>Timestamp="2025-03-17 16:43:11", LogId="1763", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="Auditing log end", ReceptionTime="2025-03-17 16:44:29", SenderType="Firewall", SituationId="78022", Situation="System_Engine-Log-Auditing-State", EventId="7307441384431027939"</pre>
FAU_GEN.1.1 c)	
Auditable event	Administrative login and logout

FAU_GEN.1.1 c)	
Administrative login	<pre>Timestamp="2025-03-17 16:48:05", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login succeeded for user test00 in domain Shared Domain", SenderType="Management Server", EventId="2665877378764374111", UserOriginator="System", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.admin.login", Result="Success", ObjectName="test00;Shared Domain"</pre>
Administrative logout	<pre>Timestamp="2025-03-17 16:51:29", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Logout succeeded for user test00.", SenderType="Management Server", EventId="2666836548040786018", UserOriginator="System", ClientIpAddress="127.0.0.1", TypeDescription="stonegate.admin.logout", Result="Success", ObjectName="test00"</pre>

FMT_SMF.1, FAU_GEN.1.1 c)	
Auditable event	Security related configuration changes
Audit server configuration changes	<pre>Timestamp="2025-04-01 17:18:27", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A new log forward rule was created with All Log Data types to host syslog_server (port 2055).", SenderType="Management Server", EventId="8239535049569992843", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.log.forward.new", Result="Success", ObjectName="Management Server"</pre> <pre>Timestamp="2025-04-01 17:18:27", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A log forward rule was deleted.", SenderType="Management Server", EventId="8239535049569992844", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.log.forward.deleted", Result="Success", ObjectName="Management Server"</pre>

FMT_SMF.1, FAU_GEN.1.1 c)

Configuring reference
identifier for the peer

```
Timestamp="2025-02-14 13:40:53",  
NodeId="192.0.2.2",  
CompId="Management Server",  
InfoMsg="netflow_collector has been added: <netflow_collector  
  data_context='All Log Data' netflow_collector_host_ref='syslog_server'  
  netflow_collector_port='2055' netflow_collector_service='tcp_with_tls'  
  netflow_collector_version='esm' tls_profile='Syslog TLS profile'/>.",  
SenderType="Management Server",  
EventId="337242339615441298",  
UserOriginator="test00",  
ClientIpAddress="192.0.2.1",  
TypeDescription="stonegate.object.update.details",  
Result="Success",  
ObjectName="Management Server"
```

FMT_SMF.1, FAU_GEN.1.1 c)

Modification of
administrator
accounts

```
Timestamp="2025-02-27 11:39:05",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
SenderType="Management Server",
EventId="2575083827416278967",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.admin.enginepassword.change",
Result="Success",
ObjectName="smcadmin"
```

```
Timestamp="2025-02-27 11:39:05",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
SenderType="Management Server",
EventId="2575083827416278966",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.admin.password.change",
Result="Success",
ObjectName="smcadmin"
```

```
Timestamp="2025-02-27 11:39:05",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
SenderType="Management Server",
EventId="2575083827416278965",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.insert",
Result="Success",
ObjectName="smcadmin"
```

```
Timestamp="2025-02-27 11:41:15",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="Administrator has changed for Restricted permissions.",
SenderType="Management Server",
EventId="2575083827416288532",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.admin.permission.change",
Result="Success",
ObjectName="smcadmin"
```

```
Timestamp="2025-02-27 11:43:44",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="Administrator has changed for Unrestricted permissions.",
SenderType="Management Server",
EventId="2575083827416288537",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.admin.permission.change",
Result="Success",
ObjectName="smcadmin"
```

FMT_SMF.1, FAU_GEN.1.1 c)	
Modification of administrator accounts (Continued)	<pre>Timestamp="2025-02-27 11:43:44", NodeId="192.0.2.2", CompId="cc-smca-mgmt", SenderType="Management Server", EventId="2575083827416288538", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="smcadmin"</pre>
Logon banner change	<pre>Timestamp="2025-02-27 11:47:36", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Updated Global System Property logon_banner_text to This is CC Audit Log Lab SMC running in FIPS mode.Unauthorized Access Prohibited. Copyright (c) 2025 Forcepoint.", SenderType="Management Server", EventId="2575083827416288550", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="logon_banner_text"</pre>
Minimum password length	<pre>Timestamp="2025-02-27 11:52:06", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Updated Global System Property password_character_number_minimum to 12", SenderType="Management Server", EventId="2575083827416288557", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="password_character_number_minimum"</pre>

FMT_SMF.1, FAU_GEN.1.1 c)

Remote session
timeout change

```
Timestamp="2025-02-27 11:58:07",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="Updated Global System Property gui_inactivity_max_in_min to 15",
SenderType="Management Server",
EventId="2575083827416288559",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update",
Result="Success",
ObjectName="gui_inactivity_max_in_min"
```

```
Timestamp="2025-02-27 11:59:32",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="Updated Global System Property behavior_after_reach_gui_inactivity_max
to TERMINATE_SESSION",
SenderType="Management Server",
EventId="2575083827416288561",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update",
Result="Success",
ObjectName="behavior_after_reach_gui_inactivity_max"
```

FMT_SMF.1, FAU_GEN.1.1 c)

Configure authentication failure parameters for FIA_AFL.1

```
Timestamp="2025-02-27 12:21:33",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="Updated Global System Property conf_time_login_delayed to 30",
SenderType="Management Server",
EventId="2575083827416288590",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update",
Result="Success",
ObjectName="conf_time_login_delayed"
```

```
Timestamp="2025-02-27 12:21:33",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="Created Global System Property failed_login_max_before_lockout with values 10",
SenderType="Management Server",
EventId="2575083827416288592",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.insert",
Result="Success",
ObjectName="failed_login_max_before_lockout"
```

```
Timestamp="2025-02-27 12:21:33",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="Updated Global System Property lock_out_setting to true",
SenderType="Management Server",
EventId="2575083827416288586",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update",
Result="Success",
ObjectName="lock_out_setting"
```

```
Timestamp="2025-02-27 12:21:33",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="Updated Global System Property max_failed_logins_per_source_before_delay to 3",
SenderType="Management Server",
EventId="2575083827416288587",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update",
Result="Success",
ObjectName="max_failed_logins_per_source_before_delay"
```

```
Timestamp="2025-02-27 12:21:33",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="Updated Global System Property failed_auth_attempt_before_delay to 5",
SenderType="Management Server",
EventId="2575083827416288589",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update",
Result="Success",
ObjectName="failed_auth_attempt_before_delay"
```

```
Timestamp="2025-02-27 12:21:33",
NodeId="192.0.2.2",CompId="cc-smca-mgmt",
InfoMsg="Updated Global System Property conf_time_all_login_per_source_delayed to 15",
SenderType="Management Server",
EventId="2575083827416288588",UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
```

FMT_SMF.1, FAU_GEN.1.1 c)	
Configure authentication failure parameters for FIA_AFL.1 (Continued)	<pre>Timestamp="2025-02-27 12:21:33", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Updated Global System Property conf_time_all_login_per_source_delayed to 15", SenderType="Management Server", EventId="2575083827416288588", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="conf_time_all_login_per_source_delayed"</pre> <pre>Timestamp="2025-02-27 12:21:33", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Created Global System Property conf_period_for_failed_login_before_lock with values 60", SenderType="Management Server", EventId="2575083827416288591", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="conf_period_for_failed_login_before_lock"</pre> <pre>Timestamp="2025-03-05 23:05:02", NodeId="192.0.2.2", CompId="cc-smca-mgmt", SenderType="Management Server", EventId="7530035494839648441", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.admin.disabled", Result="Success", ObjectName="smcadmin"</pre>
Auditable event	Configuration of time
Configuration of a new time server	<pre>Timestamp="2025-03-06 14:20:13", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="ntp_server element has been created.", SenderType="Management Server", EventId="7765054971405402282", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="cc-audit-ntp"</pre>
Auditable event	Configuration of the cryptographic functionality

FMT_SMF.1, FAU_GEN.1.1 c)

Configure the cryptographic functionality for TLS

```
Timestamp="2025-03-06 14:43:58",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="tls_cryptography_suite_set element has been created.",
SenderType="Management Server",
EventId="7765054971405402348",
UserOriginator="priadmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.insert",
Result="Success",
ObjectName="CC TLS Suite"
```

```
Timestamp="2025-03-07 12:02:33",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="tls_cryptography_suites has been modified on its attribute:
  tls_ecdhe_rsa_with_aes_128_cbc_sha (true -> false).",
SenderType="Management Server",
EventId="7765054971405403576",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="CC TLS Suite"
```

```
Timestamp="2025-03-07 12:02:33",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
SenderType="Management Server",
EventId="7765054971405403577",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update",
Result="Success",
ObjectName="CC TLS Suite"
```

```
Timestamp="2025-03-07 12:11:54",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="web_app (webswing) has been modified on its attribute: tls_cipher_suites
  (Forcepoint Approved (v1) TLS Cryptographic Algorithms -> CC TLS Suite).",
SenderType="Management Server",
EventId="7765054971405403606",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="cc-smca-mgmt"
```

FMT_SMF.1, FAU_GEN.1.1 c)

Configure the cryptographic functionality for TLS (continued)

```
Timestamp="2025-03-07 15:06:19",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="tls_cryptography_suite_set_ref has been modified (NIST (SP 800-52 Rev.
2) Compatible TLS Cryptographic Algorithms -> CC TLS Suite).",
SenderType="Management Server",
EventId="7765054971405404028",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="Audit Syslog TLS Profile"
```

```
Timestamp="2025-03-07 15:06:19",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
SenderType="Management Server",
EventId="7765054971405404029",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update",
Result="Success",
ObjectName="Audit Syslog TLS Profile"
```

```
Timestamp="2025-03-14 11:43:38",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="netflow_collector has been modified on its attribute: tls_profile (No
value -> Audit Syslog TLS Profile).",
SenderType="Management Server",
EventId="803323531923297561",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="cc-smca-mgmt"
```

```
Timestamp="2025-03-14 11:43:38",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="netflow_collector has been modified on its attribute:
netflow_collector_service (tcp -> tcp_with_tls).",
SenderType="Management Server",
EventId="803323531923297562",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="cc-smca-mgmt"
```

```
Timestamp="2025-03-14 11:43:38",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="netflow_collector has been modified on its attribute: tls_identity (No
value -> IP Address / 192.0.2.101).",
SenderType="Management Server",
EventId="803323531923297563",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="cc-smca-mgmt"
```

FMT_SMF.1, FAU_GEN.1.1 c)	
Configure the cryptographic functionality for NTP	<pre>Timestamp="2025-03-06 14:46:58", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="ntp_auth_key_type has been modified (none -> SHA1).", SenderType="Management Server", EventId="7765054971405402359", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="cc-audit-ntp"</pre> <pre>Timestamp="2025-03-06 14:46:58", NodeId="192.0.2.2", CompId="cc-smca-mgmt", SenderType="Management Server", EventId="7765054971405402360", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="cc-audit-ntp"</pre>
Auditable event	Generating / import of, changing, or deleting of cryptographic keys
Creation of a TLS private key (Administration > Certificates > TLS Credentials > New TLS Credentials)	<pre>Timestamp="2025-03-17 17:23:15", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Private Key (Algorithm: ECDSA. Size: 384)", SenderType="Management Server", EventId="2674752396105613423", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.cryptographic_key.new", Result="Success", ObjectName="Management Server"</pre>
Certificate signing request	<pre>Timestamp="2025-03-17 16:52:37", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Management Server certificate signing request was exported. The fingerprint is 5D:A2:1E:B5:EE:E9:17:9C:2F:3C:5E:AA:F5:48:CA:A3:26:16:30:88.", SenderType="Management Server", EventId="2666836548040786061", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.certificaterequest.export", Result="Success", ObjectName="Management Server"</pre>

FMT_SMF.1, FAU_GEN.1.1 c)	
Import signed certificate	<pre>Timestamp="2025-03-17 16:51:11", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="CN=LogServer 192.0.2.2: Algorithm EC. Key size 384. Validity Tue Apr 15 16:51:10 GMT 2025", SenderType="Management Server", EventId="2666836548040785992", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.certificate.import", Result="Success", ObjectName="LogServer 192.0.2.2"</pre>
Deletion (from Trash)	<pre>Timestamp="2025-02-14 13:41:09", NodeId="192.0.2.2", CompId="Management Server", EventId="338060036964089860", OriginName="MgtServer Tool", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="stonegate.cryptographic_key.deleted", Result="Success", ObjectName="Management Server"</pre>

FMT_SMF.1, FAU_GEN.1.1 c)

Import of a trusted
certificate authority
(CA)

```
Timestamp="2025-03-17 16:45:08",
NodeId="192.0.2.2",
CompId="Management Server",
SenderType="Management Server",
EventId="2663570813822697742",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.ca.internal.trust.start",
Result="Success",
ObjectName=" [0] Version: 3 SerialNumber:
290537198474842792658101195459566188220737020075
IssuerDN: CN=ext_pki-styx-ca certificate L=Helsinki C=FI Start Date:
Mon Mar 17 16:45:07 GMT 2025
Final Date: Thu Sep 28 16:45:07 GMT 2045
SubjectDN: CN=ext_pki-styx-ca certificate L=Helsinki C=FI
Public Key: EC Public Key
[7a:ce:6c:f3:43:68:df:09:2b:e1:b7:82:5e:e8:f9:28:75:a8:f8:dc]
X: 1c25b5a47d5cde5ecfa5283dc248985956c748a6b4703f109689ada67
d951fb5778d0cdf2bbbc590306d21de761489b
Y: c6ec13c2cbd9675934b675f2c8a0f5cedf7458af4d23a20c77048ccdd
c0670035518ef4f4a25b461197083c5046f6834
Signature Algorithm: SHA384WITHECDSA Signature:
3064023024052c2cc1bbfddb1ab9022d0db6d115
5cbc03339c7f7d6c4086ec461e641abe8ce4e3ad
9c150b2304fb4cc37bfda30d0230645287efa16d
4a8fdbd5ee3e19331c6b6a32493c66697b586363
24ca541263cd611c57cb75257ff3f257f8b7a7b8
d99d Extensions: critical(false) 2.5.29.14 value =
DER Octet String[20]
critical(true) BasicConstraints: isCa(true) critical(true)
KeyUsage: 0x86"
```

```
Timestamp="2025-03-17 16:45:08",
NodeId="192.0.2.2",
CompId="Management Server",
SenderType="Management Server",
EventId="2663570813822697743",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.ca.internal.trust.start",
Result="Success",
ObjectName="CN=ext_pki-styx-ca certificate L=Helsinki C=FI"
```

FMT_SMF.1, FAU_GEN.1.1 c)

Import of a private
key and a certificate

```
Timestamp="2025-03-18 10:50:36",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="Cryptographic key imported",
SenderType="Management Server",
EventId="2939203183311848077",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.cryptographic_key.import",
Result="Success",
ObjectName="example_creds"
```

```
Timestamp="2025-03-18 10:50:36",
NodeId="192.0.2.2",
CompId="Management Server",
SenderType="Management Server",
EventId="2939203183311848078",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.certificate.import",
Result="Success",
ObjectName="example_creds"
```

```
Timestamp="2025-03-18 10:50:36",
NodeId="192.0.2.2",
CompId="Management Server",
SenderType="Management Server",
EventId="2939203183311848079",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.insert",
Result="Success",
ObjectName="example_creds"
```

FMT_SMF.1, FAU_GEN.1.1 c)	
Removal (Deletion) of a Trusted Certificate Authority	<pre>Timestamp="2025-03-18 11:06:54", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="2939203183311848443", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.delete", Result="Success", ObjectName="example_trustedCA"</pre> <pre>Timestamp="2025-03-18 11:06:54", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="2939203183311848444", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.cryptographic_key.deleted", Result="Success", ObjectName="example_trustedCA"</pre> <pre>Timestamp="2025-03-18 11:06:54", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Certificate of a Certificate Authority with subject name CN=intermCA OU=Silicon O=Forcepoint L=Helsinki ST=Uusimaa C=FI.", SenderType="Management Server", EventId="2939203183311848445", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.certificate.delete", Result="Success"</pre>
Auditable event	Resetting passwords
Password reset	<pre>Timestamp="2025-03-14 13:16:38", NodeId="192.0.2.2", CompId="cc-smca-mgmt", SenderType="Management Server", EventId="803323531923297856", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.admin.enginepassword.change", Result="Success", ObjectName="smcadmin"</pre> <pre>Timestamp="2025-03-14 13:16:38", NodeId="192.0.2.2", CompId="cc-smca-mgmt", SenderType="Management Server", EventId="803323531923297855", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.admin.password.change", Result="Success", ObjectName="smcadmin"</pre>

FCS_NTP_EXT.1, FAU_GEN.1.1 c)

Configuration of a new time server

```
Timestamp="2025-03-14 13:35:25",
NodeId="192.0.2.2",CompId="cc-smca-mgmt",
InfoMsg="ntp_server_ref has been added: <ntp_server_ref ref='cc-ntp-2'/>.",
SenderType="Management Server",
EventId="803323531923297906",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="cc-ngfw"
```

```
Timestamp="2025-03-14 13:35:25",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="ntp_settings has been modified on its attribute:
ntp_preferred_server_ref (No value -> cc-ntp-2).",
SenderType="Management Server",
EventId="803323531923297905",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="cc-ngfw"
```

FCS_NTP_EXT.1, FAU_GEN.1.1 c)

Removal of
configured time
server

```
Timestamp="2025-03-14 13:38:13",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="ntp_server_ref has been removed: <ntp_server_ref ref='cc-ntp-2'/>.",
SenderType="Management Server",
EventId="803323531923297915",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="cc-ngfw"
```

```
Timestamp="2025-03-14 13:38:13",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="ntp_settings has been modified on its attribute:
  ntp_preferred_server_ref (cc-ntp-2 -> No value).",
SenderType="Management Server",
EventId="803323531923297914",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="cc-ngfw"
```

```
Timestamp="2025-03-14 13:40:01",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
SenderType="Management Server",
EventId="803323531923297919",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.trash.add",
Result="Success",
ObjectName="cc-ntp-2"
```

```
Timestamp="2025-03-14 13:40:14",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
SenderType="Management Server",
EventId="803323531923297921",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.delete",
Result="Success",
ObjectName="cc-ntp-2"
```

Manual time change

```
Timestamp="2025-03-17 11:50:55",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Mar 17 11:50:55 cc-audit-smca sudo: radmin : TTY=ttty1 ; PWD=/home/
radmin ; USER=root ; COMMAND=/bin/date -s 'Mar 17 11:55:55 UTC 2025'",
ReceptionTime="2025-03-17 11:50:55",
SenderType="Third Party Device",
EventId="72"
```

FMT SMF.1/FFW FAU_GEN.1.1 c)	
Engine filtering rule change	<pre> Timestamp="2025-03-17 17:10:07", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="rule_entry (@134.1) has been modified on its attribute: is_disabled (false -> true).", SenderType="Management Server", EventId="2670690370655879358", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Allow FTP and SSH" </pre>
Engine security policy change	<pre> Timestamp="2025-03-17 17:10:08", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Upload started from REST API", SenderType="Management Server", EventId="2670690370655879363", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.policy.upload.start", Result="Success", ObjectName="Allow FTP and SSH policy;ngfw" </pre> <pre> Timestamp="2025-03-17 17:10:25", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Upload started from REST API", SenderType="Management Server", EventId="2670690370655879370", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.policy.upload.end", Result="Success", ObjectName="Allow FTP and SSH policy;ngfw" </pre>

FMT SMF.1/FFW FAU_GEN.1.1 c)

Engine security policy
change
(add rule)

```
Timestamp="2025-03-17 17:10:07",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="access_entry has been added: <rule_entry is_disabled='false'
parent_rule_ref='Access rule : insert point' rank='1.0'
tag='132.0'><match_part><match_sources><match_source_ref type='network_element'
value='ANY'></match_sources><match_destinations><match_destination_ref
type='network_element' value='ANY'></match_destinations><match_services><match_service_ref
type='application' value='FTP'></match_services></match_part><option><log_policy closing_mode='true' log_level='undefined'
mss_enforce='false'><payload_modes><payload_mode type='string' value='nothing'></payload_modes></log_policy></option></rule_entry>.",
SenderType="Management Server",
EventId="2670690370655879346",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="Allow FTP and SSH"
```

```
Timestamp="2025-03-17 17:10:07",
NodeId="192.0.2.2",
CompId="Management Server",
SenderType="Management Server",
EventId="2670690370655879350",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update",
Result="Success",
ObjectName="Allow FTP and SSH"
```

FMT SMF.1/FFW FAU_GEN.1.1 c)

Engine security policy
change
(delete rule)

```
Timestamp="2025-03-18 13:45:04",
NodeId="192.0.2.2",
RuleId="134.1",
CompId="Management Server",
InfoMsg="IPv4 Access @134.1 has been deleted.",
SenderType="Management Server",
EventId="2987302565009424679",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.delete",
Result="Success",
ObjectName="Allow FTP and SSH policy"
```

```
Timestamp="2025-03-18 13:45:04",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="rule_entry (@134.1) has been removed: <rule_entry
name='discard all' is_disabled='true' parent_rule_ref='Access
rule : insert point' rank='-50.0' rule_tag_major_id='134'
tag='134.1'><match_part><match_sources><match_source_ref type='network_element'
value='ANY'/></match_sources><match_destinations><match_destination_ref
type='network_element' value='ANY'/></
match_destinations><match_services><match_service_ref type='service' value='ANY'/
></match_services></match_part><option><log_policy closing_mode='true'
log_level='undefined' mss_enforce='false'><payload_modes><payload_mode
type='string' value='nothing'/></payload_modes></log_policy></option></
rule_entry>.",
SenderType="Management Server",
EventId="2987302565009424680",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="Allow FTP and SSH policy"
```

Engine security policy
change
(create policy)

```
Timestamp="2025-03-17 17:10:06",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="fw_policy element has been created.",
SenderType="Management Server",
EventId="2670690370655879343",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.insert",
Result="Success",
ObjectName="Allow FTP and SSH"
```

FMT SMF.1/FFW FAU_GEN.1.1 c)	
Engine security policy change (upload policy)	<pre>Timestamp="2025-03-17 17:10:08", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Upload started from REST API", SenderType="Management Server", EventId="2670690370655879363", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.policy.upload.start", Result="Success", ObjectName="Allow FTP and SSH policy;ngfw"</pre> <pre>Timestamp="2025-03-17 17:10:25", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="2670690370655879369", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.firewall.policy.upload", Result="Success", ObjectName="ngfw;Allow FTP and SSH policy"</pre> <pre>Timestamp="2025-03-17 17:10:25", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Upload started from REST API", SenderType="Management Server", EventId="2670690370655879370", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.policy.upload.end", Result="Success", ObjectName="Allow FTP and SSH policy;ngfw"</pre>
Firewall security policy change (delete policy)	<pre>Timestamp="2025-03-17 17:10:34", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="2670690370655879373", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.delete", Result="Success", ObjectName="Allow FTP and SSH policy"</pre>

FMT_SMF.1/VPN, FAU_GEN.1.1 c) VPN security policy change**VPN security policy change (adding rule)**

```
Timestamp="2025-03-26 14:47:31",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="rule_entry (@123.0) has been added: <rule_entry name='discard
ISAKMP and NAT-T' is_disabled='false' parent_rule_ref='Access
rule : insert point' rank='-25.0' rule_tag_major_id='123'
tag='123.0'><match_part><match_sources><match_source_ref type='network_element'
value='ANY'/></match_sources><match_destinations><match_destination_ref
type='network_element' value='$$ Local Cluster'/></match_destinations><match_services><match_service_ref type='application'
value='ISAKMP'/><match_service_ref type='application' value='NAT-
T'/></match_services><rule_validity_times><rule_validity_time_ref
type='rule_validity_time' value='Weekends'/></rule_validity_times></
match_part><option><log_policy closing_mode='true' log_level='undefined'
mss_enforce='false'><payload_modes><payload_mode type='string' value='nothing'/
></payload_modes></log_policy></option></rule_entry>.",
SenderType="Management Server",
EventId="5973932190247944426",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="auditpolicy"
```

```
Timestamp="2025-03-26 14:47:31",
NodeId="192.0.2.2",
RuleId="123.0",
CompId="Management Server",
InfoMsg="IPv4 Access @123.0 has been added.",
SenderType="Management Server",
EventId="5973932190247944425",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.insert",
Result="Success",
ObjectName="auditpolicy"
```

VPN security policy change (modify rule)

```
Timestamp="2025-03-26 14:47:33",
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="5973932190247944430",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="auditpolicy"
```

```
Timestamp="2025-03-26 14:47:33",
NodeId="192.0.2.2",
RuleId="123.1",
CompId="Management Server",
InfoMsg="IPv4 Access @123.1 has been modified.",
SenderType="Management Server",
EventId="5973932190247944428",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update",
Result="Success",
ObjectName="auditpolicy"
```

FMT_SMF.1/VPN, FAU_GEN.1.1 c) VPN security policy change

VPN security policy change (delete rule)

```
Timestamp="2025-03-26 14:47:35",
NodeId="192.0.2.2",RuleId="123.1",
CompId="Management Server",
InfoMsg="IPv4 Access @123.1 has been deleted.",
SenderType="Management Server",
EventId="5973932190247944432",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.delete",
Result="Success",
ObjectName="auditpolicy"
```

```
Timestamp="2025-03-26 14:47:38",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="rule_entry (@123.1) has been removed: <rule_entry name='discard
ISAKMP and NAT-T' is_disabled='false' parent_rule_ref='Access
rule : insert point' rank='-25.0' rule_tag_major_id='123'
tag='123.1'><match_part><match_sources><match_source_ref
type='network_element' value='network-192.0.2.0/24'></
match_sources><match_destinations><match_destination_ref
type='network_element' value='$$ Local Cluster'></
match_destinations><match_services><match_service_ref type='application'
value='ISAKMP'></match_service_ref type='application' value='NAT-
T'></match_services><rule_validity_times><rule_validity_time_ref
type='rule_validity_time' value='Weekends'></rule_validity_times></
match_part><option><log_policy closing_mode='true' log_level='undefined'
mss_enforce='false'><payload_modes><payload_mode type='string' value='nothing'>
</payload_modes></log_policy></option></rule_entry>.",
SenderType="Management Server",
EventId="5973932190247944434",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="auditpolicy"
```

FPT_STM_EXT.1	
NTP time change	<pre>Timestamp="2025-04-07 13:55:52", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Apr 7 13:55:52 cc-smca chronyd[290768]: Backward time jump detected!", ReceptionTime="2025-04-07 13:55:52", SenderType="Third Party Device", EventId="11456"</pre> <pre>Timestamp="2025-04-07 15:14:14", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Apr 7 15:14:14 cc-smca chronyd[290768]: System clock was stepped by 4571.600739 seconds", ReceptionTime="2025-04-07 15:14:14", SenderType="Third Party Device", EventId="11460"</pre> <pre>Timestamp="2025-04-07 16:15:53", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Apr 7 16:15:53 cc-smca chronyd[290768]: Forward time jump detected!", ReceptionTime="2025-04-07 16:15:53", SenderType="Third Party Device", EventId="11540"</pre>
NTP time change (Continued)	<pre>Timestamp="2025-04-07 15:17:29", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Apr 7 15:17:29 cc-smca chronyd[290768]: System clock was stepped by -3634.485642 seconds", ReceptionTime="2025-04-07 15:17:29", SenderType="Third Party Device", EventId="11544"</pre> <pre>Timestamp="2025-04-08 12:48:41", LogId="818214", NodeId="192.0.2.4", Facility="Syslog", Type="Notification", CompId="cc-ngfw-1 node 1", InfoMsg="ntpd: Time change. Before: Tue Apr 8 12:44:08 After: Tue Apr 8 12:48:41 Peer: 192.0.2.123", ReceptionTime="2025-04-08 12:48:47", SenderType="Firewall", EventId="7315354900329430054"</pre>
FCS_TLSC_EXT.1	
Auditable event	TLS client sessions

FCS_TLSC_EXT.1	
Failure to establish a TLS client session	<pre>Timestamp="2025-03-14 11:55:05", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.10 port=2055] Local = [host=192.0.2.2 port=35696] ERROR: Syslog authentication failed. [/192.0.2.10:2055] Details: certificate expired on 20200102080000GMT +00:00", SenderType="Management Server", EventId="1476204865502838960", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>

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	<pre>Timestamp="2025-03-18 13:44:04", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.1 port=57556] Local = [host=192.0.2.2 port=8085]", SenderType="Management Server", EventId="2987302565009424613", UserOriginator="System", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.trusted.connection.start", Result="Success"</pre>
Termination of an HTTPS or TLS session, or trusted path	<pre>Timestamp="2025-03-18 13:45:06", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.1 port=57556] Local = [host=192.0.2.2 port=8085]", SenderType="Management Server", EventId="2987302565009424682", UserOriginator="System", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.trusted.connection.end", Result="Success"</pre>
Failure to establish an HTTPS or TLS session, or trusted path	<pre>Timestamp="2025-03-17 17:38:24", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.2 port=36208] Local = [host=192.0.2.2 port=3023] ERROR: Communication authentication failed. [192.0.2.2:36208] Details: Failed to check certificate Certificate Error: KeyUsage extension not present in CA certificate", SenderType="Management Server", EventId="2675169377300513405", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>

FCS_TLSS_EXT.2	
Auditable event	TLS sessions
Failure to authenticate the client (SMC as a server)	<pre>Timestamp="2025-03-17 16:51:33", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.2 port=39142] Local = [host=192.0.2.2 port=3023] ERROR: Communication authentication failed. [192.0.2.2:39142] Details: Failed to check certificate Certificate Error: The Certificate (subjectDN=CN=ext_pki-ocsp-ic certificate C=FI serialNumber=1): Certificate has been revoked reason: KEY_COMPROMISE revocation date: Mon Mar 17 16:50:27 GMT 2025 authority: CN=ext_pki-ocsp-ca certificate L=Helsinki C=FI extension OIDs: []", SenderType="Management Server", EventId="2665307750136807714", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>
Failure to authenticate the client (Security Engine as a server)	<pre>Timestamp="2025-03-17 17:22:53", LogId="1975", NodeId="192.0.2.4", Facility="Management", Type="Error", CompId="ngfw node 1", InfoMsg="peer did not return a certificate", ReceptionTime="2025-03-17 17:22:54", SenderType="Firewall", SituationId="9005", Situation="FW_Communication-Communication-Error", EventId="7307451370229991351"</pre> <pre>Timestamp="2025-03-17 17:22:53", LogId="1976", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="TLS: Couldn't accept TLS connection: -3 (DNS:ManagementServer 192.0.2.2)", ReceptionTime="2025-03-17 17:22:54", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="7307451370229991352"</pre>

FFW_RUL_EXT.1	
Half-open connection limit	<pre>Timestamp="2025-03-27 12:22:46", LogId="2693", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Dst="203.0.113.6", CompId="ngfw node 1", InfoMsg="Protection started Trigger: half-open limit", ReceptionTime="2025-03-27 12:22:47", SenderType="Firewall", SituationId="79990", Situation="DOS_SYN-Flood-Started", EventId="7310999726181057677"</pre>
Auditable event	Application of rules configured with the 'log' operation
Connection allowed	<pre>Timestamp="2025-03-18 13:37:46", LogId="884", NodeId="192.0.2.4", Facility="Inspection", Type="Notification", Event="New connection", Action="Allow", Protocol="6", Src="198.51.100.6", Dst="203.0.113.6", Sport="44484", Dport="21", RuleId="132.0", Srcif="1", CompId="ngfw node 1", ReceptionTime="2025-03-18 13:37:47", SenderType="Firewall", SituationId="70018", Situation="Connection_Allowed", EventId="7307757111144186405", Service="FTP"</pre>
Connection discarded	<pre>Timestamp="2025-03-17 17:10:19", LogId="871", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="Connection discarded", Action="Discard", Protocol="58", Src="::16", Dst="FF02::16", RuleId="46.0", Srcif="0", IcmpType="143", IcmpCode="0", CompId="ngfw node 1", ReceptionTime="2025-03-17 17:10:20", SenderType="Firewall", SituationId="70019", Situation="Connection_Discarded", EventId="7307448209134059546", Service="IPv6 ICMP/143/0"</pre>

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> Timestamp="2025-03-17 17:10:33", LogId="932", NodeId="192.0.2.4", Facility="Inspection", Type="Notification", Event="New connection", Action="Allow", Protocol="6", Src="198.51.100.6", Dst="203.0.113.6", Sport="51142", Dport="21", RuleId="132.0", Srcif="1", CompId="ngfw node 1", ReceptionTime="2025-03-17 17:10:34", SenderType="Firewall", SituationId="70018", Situation="Connection_Allowed", EventId="7307448268685485565", Service="FTP" </pre> <pre> Timestamp="2025-03-17 17:10:33", LogId="934", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="Related connection", Action="Allow", Protocol="6", Src="198.51.100.6", Dst="203.0.113.6", Sport="46660", Dport="51332", RuleId="132.0", Srcif="1;1", CompId="ngfw node 1", ReceptionTime="2025-03-17 17:10:34", SenderType="Firewall", SituationId="1004", Situation="FW_Related-Connection", EventId="7307448264968634400", Service="TCP/51332" </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	<pre>Timestamp="2025-03-17 02:38:50", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Too many login failures in 30 mins account is disabled. 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="803323531923306073", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="stonegate.admin.disabled", Result="Fail", ObjectName="secadmin"</pre> <pre>Timestamp="2025-03-17 02:35:09", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Too many login failures from same source wait 30 min 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="803323531923306004", UserOriginator="System", ClientIpAddress="192.168.200.10", TypeDescription="stonegate.admin.login", Result="Fail", ObjectName="Unknown user"</pre>
FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Auditable event	All use of identification and authentication mechanism
Local session identification and authentication failures	<pre>Timestamp="2025-03-23 12:34:35", NodeId="127.0.0.1",Type="Notification", CompId="3", InfoMsg="Mar 23 12:34:35 cc-audit-smca login: pam_unix(login:auth): check pass; user unknown", ReceptionTime="2025-03-23 12:34:35", SenderType="Third Party Device", EventId="11720"</pre> <pre>Timestamp="2025-03-23 12:34:35", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Mar 23 12:34:35 cc-audit-smca login: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost=", ReceptionTime="2025-03-23 12:34:35", SenderType="Third Party Device", EventId="11721"</pre>

FIA_UAU_EXT.2, FIA_UIA_EXT.1

Local session
identification and
authentication failures
(continue)

```
Timestamp="2025-03-23 12:34:35",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Mar 23 12:34:35 cc-audit-smca login: pam_faillock(login:auth): User
unknown",
ReceptionTime="2025-03-23 12:34:35",
SenderType="Third Party Device",
EventId="11722"
```

```
Timestamp="2025-03-23 12:34:36",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Mar 23 12:34:36 cc-audit-smca login: FAILED LOGIN SESSION FROM tty1 FOR
nadmin Permission denied",
ReceptionTime="2025-03-23 12:34:36",
SenderType="Third Party Device",
EventId="11724"
```

Local session
identification and
authentication failures
(Continued)

```
Timestamp="2025-03-23 12:43:20",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Mar 23 12:43:20 cc-audit-smca unix_chkpwd[327750]: password check failed
for user (radmin)",
ReceptionTime="2025-03-23 12:43:20",
SenderType="Third Party Device",
EventId="11738"
```

```
Timestamp="2025-03-23 12:43:20",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Mar 23 12:43:20 cc-audit-smca login: pam_unix(login:auth):
authentication failure; logname= uid=0 euid=0 tty=/dev/tty1 ruser= rhost=
user=radmin",
ReceptionTime="2025-03-23 12:43:20",
SenderType="Third Party Device",
EventId="11739"
```

```
Timestamp="2025-03-23 12:43:22",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Mar 23 12:43:22 cc-audit-smca login: FAILED LOGIN SESSION FROM tty1 FOR
radmin Permission denied",
ReceptionTime="2025-03-23 12:43:22",
SenderType="Third Party Device",
EventId="11741"
```

FIA_UAU_EXT.2, FIA_UIA_EXT.1	
Local session successful identification and authentication	<pre>Timestamp="2025-03-23 11:37:11", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Mar 23 11:37:11 cc-audit-smca login: pam_unix(login:session): session opened for user radmin(uid=1000) by radmin(uid=0)", ReceptionTime="2025-03-23 11:37:11", SenderType="Third Party Device", EventId="11465"</pre> <pre>Timestamp="2025-03-23 11:37:11", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Mar 23 11:37:11 cc-audit-smca login: LOGIN ON tty1 BY radmin", ReceptionTime="2025-03-23 11:37:11", SenderType="Third Party Device", EventId="11468"</pre>
Remote session identification and authentication failures	<pre>Timestamp="2025-03-17 02:38:50", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Login failed for user secadmin. 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="803323531923306074", UserOriginator="System", ClientIpAddress="192.168.200.10", TypeDescription="stonegate.admin.login", Result="Fail", ObjectName="secadmin;Shared Domain"</pre> <pre>Timestamp="2025-03-17 02:43:58", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Login attempt for unknown user badadmin", SenderType="Management Server", EventId="803323531923306112", UserOriginator="System", ClientIpAddress="192.168.200.10", TypeDescription="stonegate.admin.login", Result="Fail", ObjectName="Unknown user"</pre>
Remote session identification and authentication succeeds	<pre>Timestamp="2025-03-18 13:44:10", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Login succeeded for user test00 in domain Shared Domain", SenderType="Management Server", EventId="2987302565009424645", UserOriginator="System", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.admin.login", Result="Success", ObjectName="test00;Shared Domain"</pre>

FIA_X509_EXT.1	
Auditable event	Unsuccessful attempt to validate a certificate
Unsuccessful attempt to validate a certificate	<pre> Timestamp="2025-03-14 11:55:05", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Certificate validation failed.Protocol = TLSv1.2 Peer = [host=192.0.2.10 port=2055] Local = [host=Unknown port=Unknown] ERROR: certificate expired on 20200102080000GMT+00:00", SenderType="Management Server", EventId="1476204865502838959", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.certificate.validation.failure", Result="Fail" </pre> <pre> Timestamp="2025-03-14 11:55:05", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.10 port=2055] Local = [host=192.0.2.2 port=35696] ERROR: Syslog authentication failed. [/192.0.2.10:2055] Details: certificate expired on 20200102080000GMT +00:00", SenderType="Management Server", EventId="1476204865502838960", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.failure", Result="Fail" </pre> <pre> Timestamp="2025-03-19 11:19:42", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Certificate validation failed.Protocol = TLSv1.2 Peer = [host=192.0.2.10 port=2055] Local = [host=Unknown port=Unknown] ERROR: Server Identity Check Failed", SenderType="Management Server", EventId="3322506096534356246", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.certificate.validation.failure", Result="Fail" </pre> <pre> Timestamp="2025-03-19 11:19:42", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.10 port=2055] Local = [host=192.0.2.2 port=45304] ERROR: Syslog authentication failed. [/192.0.2.10:2055] Details: Server Identity Check Failed", SenderType="Management Server", EventId="3322506096534356257", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.failure", Result="Fail" </pre>
FIA_X509_EXT.1/ITT	
Auditable event	Unsuccessful attempt to validate a certificate

FIA_X509_EXT.1/ITT

Unsuccessful attempt to validate a certificate (Security Engine)

```
Timestamp="2025-03-17 17:26:54",
LogId="1876",
NodeId="192.0.2.4",
Facility="Management",
Type="Warning",
Src="192.0.2.2",
Dst="192.0.2.4",
CompId="ngfw node 1",
InfoMsg="Revocation check failed with status: enoent state: cert_revoked
path_not_verified certificate identity: Subject:C=FR CN=MgtSrvCert|Issuer:C=FI
CN=ext_pki-ocsp-ic certificate|Serial:0x1",
ReceptionTime="2025-03-17 17:26:55",
SenderType="Firewall",
SituationId="79059",
Situation="TLS_Certificate-Verify-Failed",
EventId="7307452383842273108"
```

```
Timestamp="2025-03-17 17:26:54",
LogId="1877",
NodeId="192.0.2.4",
Facility="Management",
Type="Error",
CompId="ngfw node 1",
InfoMsg="Dropping client 192.0.2.4:56999-192.0.2.2:8906 due to validation
failure",
ReceptionTime="2025-03-17 17:26:55",
SenderType="Firewall",
EventId="7307452383842273109"
```

```
Timestamp="2025-03-17 17:26:54",
LogId="1878",
NodeId="192.0.2.4",
Facility="Management",
Type="Notification",
CompId="ngfw node 1",
InfoMsg="TLS: Connection disconnect (DNS:ManagementServer 192.0.2.2)",
ReceptionTime="2025-03-17 17:26:55",
SenderType="Firewall",
SituationId="78002",
Situation="TLS connection state",
EventId="7307452383842273110"
```

```
Timestamp="2025-03-17 17:27:44",
LogId="5716",
NodeId="192.0.2.4",
Facility="Management",
Type="Warning",
Src="192.0.2.2",
Dst="192.0.2.4",
CompId="ngfw node 1",
InfoMsg="Revocation check failed with status: enoent state: cert_revoked
path_not_verified certificate identity: Subject:C=FI CN=ext_pki-ocsp-ic
certificate|Issuer:C=FI L=Helsinki CN=ext_pki-ocsp-ca certificate|Serial:0x1",
ReceptionTime="2025-03-17 17:27:44",
SenderType="Firewall",
SituationId="79059",
Situation="TLS_Certificate-Verify-Failed",
EventId="7307452590000707156"
```

FIA_X509_EXT.1/ITT	
Unsuccessful attempt to validate a certificate (Security Engine (continued)))	<pre>Timestamp="2025-03-17 17:27:44", LogId="5717", NodeId="192.0.2.4", Facility="Management", Type="Error", CompId="ngfw node 1", InfoMsg="Dropping client 192.0.2.4:54419-192.0.2.2:8906 due to validation failure", ReceptionTime="2025-03-17 17:27:44", SenderType="Firewall", EventId="7307452590000707157"</pre> <pre>Timestamp="2025-03-17 17:27:44", LogId="5718", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="TLS: Connection disconnect (DNS:ManagementServer 192.0.2.2)", ReceptionTime="2025-03-17 17:27:44", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="7307452590000707158"</pre>
Unsuccessful attempt to validate a certificate (SMC)	<pre>Timestamp="2025-03-17 16:48:14", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.2 port=57136] Local = [port=8907] ERROR: Failed to check certificate Details: Certificate Error: The Certificate (subjectDN=CN=LogServer 192.0.2.2 serialNumber=1): Certificate has been revoked reason: KEY_COMPROMISE revocation date: Mon Mar 17 16:47:51 GMT 2025 authority: CN=OCSP Responder L=Helsinki C=FI extension OIDs: []", SenderType="Management Server", EventId="2665307750136807579", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>
FMT_MOF.1/ManualUpdate	
Auditable event	Any attempt to initiate a manual update

FMT_MOF.1/ManualUpdate

Any attempt to initiate a manual update

```
Timestamp="2025-03-17 03:31:03",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
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="803323531923306234",
UserOriginator="smcoperator",
ClientIpAddress="192.168.200.10",
TypeDescription="stonegate.mgtserver.upgrade.import",
Result="Fail",
ObjectName="Engine Upgrade sg_engine_7.3.0.31055_x86-64-small.zip"
```

```
Timestamp="2025-07-08 12:15:39",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
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="7625591619458170908",
UserOriginator="smcoperator",
ClientIpAddress="192.168.200.10",
TypeDescription="stonegate.mgtserver.appliance_patch.import",
Result="Fail",
ObjectName="SMC Appliance Patch 7.3.1U001.sap"
```

FMT_MOF.1/Functions

Auditable event

Modification of the behavior of the audit functionality when Local Audit Storage Space is full

Modification of the behavior of the audit functionality when Local Audit Storage Space is full

```
Timestamp="2025-03-17 02:55:20",
NodeId="192.0.2.2",
CompId="cc-smca-mgmt",
InfoMsg="log_disk_space_handling_mode has been modified (overwrite_oldest ->
stop_receiving).",
SenderType="Management Server",
EventId="803323531923306136",
UserOriginator="radmin",
ClientIpAddress="192.168.200.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="cc-smca-mgmt"
```

FMT_MOF.1/Functions	
Modification of the behavior of the transmission of audit data to an external IT entity	<pre>Timestamp="2025-03-17 16:57:55", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="A new log forward rule was created with types to host syslog_server (port 2055).", SenderType="Management Server", EventId="2665307750136807974", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.log.forward.new", Result="Success", ObjectName="Management Server"</pre>
Modification of the behavior of the handling of audit data	<pre>Timestamp="2025-03-17 03:04:50", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="storable_task_definition element has been created.", SenderType="Management Server", EventId="803323531923306146", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="Delete old Audit data"</pre> <pre>Timestamp="2025-03-17 03:06:22", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="task_schedule element has been created.", SenderType="Management Server", EventId="803323531923306147", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="(Schedule) Delete old Audit data"</pre>
FPT_ITT.1	
Auditable event	TLS communication between the distributed TOE components
Initiation of the trusted channel (Security Engine)	<pre>Timestamp="2025-03-17 16:40:31", LogId="2808", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="TLS: Accepted connection (DNS:ManagementServer 192.0.2.2)", ReceptionTime="2025-03-17 16:40:32", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="7307440710121163512"</pre>

FPT_ITT.1	
Termination of the trusted channel (Security Engine)	<pre>Timestamp="2025-03-17 16:40:44", LogId="2822", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="TLS: Connection closed (DNS:ManagementServer 192.0.2.2)", ReceptionTime="2025-03-17 16:40:45", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="7307440765955738374"</pre>
Failure of the trusted channel functions (Security Engine)	<pre>Timestamp="2025-03-17 17:22:56", LogId="1981", NodeId="192.0.2.4", Facility="Management", Type="Error", CompId="ngfw node 1", InfoMsg="no shared cipher", ReceptionTime="2025-03-17 17:22:57", SenderType="Firewall", SituationId="9005", Situation="FW_Communication-Communication-Error", EventId="7307451383114893245"</pre> <pre>Timestamp="2025-03-17 17:22:56", LogId="1982", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="TLS: Couldn't accept TLS connection: -3 (DNS:ManagementServer 192.0.2.2)", ReceptionTime="2025-03-17 17:22:57", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="7307451383114893246"</pre>
Initiation of the trusted channel (SMC)	<pre>Timestamp="2025-03-18 13:37:40", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=49771] Local = [host=192.0.2.2 port=8906]", SenderType="Management Server", EventId="2987302565009424590", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.start", Result="Success"</pre>

FPT_ITT.1

Termination of the trusted channel (SMC)

```
Timestamp="2025-03-18 13:37:40",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.4
port=49771] Local = [port=8906]",
SenderType="Management Server",
EventId="2987302565009424593",
UserOriginator="System",
ClientIpAddress="192.0.2.4",
TypeDescription="stonegate.trusted.connection.end",
Result="Success"
```

Failure of the trusted channel functions (SMC)

```
Timestamp="2025-03-17 16:57:48",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.2
port=54902] Local = [port=8907] ERROR: Failed to check certificate Details:
Certificate Error: The Certificate (subjectDN=CN=LogServer 192.0.2.2
serialNumber=4): Responder's certificate not valid for signing OCSP responses",
SenderType="Management Server",
EventId="2665307750136807967",
UserOriginator="System",
ClientIpAddress="192.0.2.2",
TypeDescription="stonegate.trusted.connection.failure",
Result="Fail"
```

FPT_TUD_EXT.1

Auditable event

Initiation of update

Verification of image (SMC)

```
Timestamp="2025-07-11 08:42:45",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 11 08:42:45 cc-smca AMBR_LOGGER.log : INFO : pid=2482 : Verified
patch 7.3.0U001.",
ReceptionTime="2025-07-11 08:42:45",
SenderType="Third Party Device",
EventId="2762"
```

FPT_TUD_EXT.1	
SMC Appliance update	<pre>Timestamp="2025-07-11 10:06:27", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Jul 11 10:06:27 cc-smca sudo: sgadmin : PWD=/usr/local/forcepoint/smc ; USER=radmin ; GROUP=smca_priv ; COMMAND=/usr/bin/sudo /usr/bin/ambr-load -f / usr/local/forcepoint/smc/7.3.0U001.sap", ReceptionTime="2025-07-11 10:06:27", SenderType="Third Party Device", EventId="3241"</pre> <pre>Timestamp="2025-07-11 10:06:27", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Jul 11 10:06:27 cc-smca sudo: radmin : PWD=/usr/local/forcepoint/ smc ; USER=root ; COMMAND=/usr/bin/ambr-load -f /usr/local/forcepoint/ smc/7.3.0U001.sap", ReceptionTime="2025-07-11 10:06:27", SenderType="Third Party Device", EventId="3269"</pre>

FPT_TUD_EXT.1

Successful SMC
update

```
Timestamp="2025-07-11 11:03:16",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 11 11:03:16 cc-smca sudo: radmin : TTY=tty1 ; PWD=/home/radmin ;
USER=root ; COMMAND=/usr/bin/ambr-install --no-prompt 7.3.0U001",
ReceptionTime="2025-07-11 11:03:16",
SenderType="Third Party Device",
EventId="3462"
```

```
Timestamp="2025-07-11 11:03:57",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 11 11:03:57 cc-smca AMBR_LOGGER.log : INFO : pid=7527 : Verified
patch 7.3.0U001.",
ReceptionTime="2025-07-11 11:03:57",
SenderType="Third Party Device",
EventId="3466"
```

```
Timestamp="2025-07-11 11:03:57",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 11 11:03:57 cc-smca AMBR_LOGGER.log : INFO : pid=7527 : Creating
recovery snapshot...",
ReceptionTime="2025-07-11 11:03:57",
SenderType="Third Party Device",
EventId="3467"
```

```
Timestamp="2025-07-11 11:03:58",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 11 11:03:58 cc-smca AMBR_LOGGER.log : INFO : pid=7527 : Created
recovery snapshot.",
ReceptionTime="2025-07-11 11:03:58",
SenderType="Third Party Device",
EventId="3474"
```

```
Timestamp="2025-07-11 11:03:58",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 11 11:03:58 cc-smca AMBR_LOGGER.log : INFO : pid=7527 : Creating
configuration backup...",
ReceptionTime="2025-07-11 11:03:58",
SenderType="Third Party Device",
EventId="3475"
```

```
Timestamp="2025-07-11 11:04:26",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 11 11:04:26 cc-smca AMBR_LOGGER.log : INFO : pid=7527 : Created
configuration backup.",
ReceptionTime="2025-07-11 11:04:26",
SenderType="Third Party Device",
EventId="3494"
```

```
Timestamp="2025-07-11 11:04:26",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 11 11:04:26 cc-smca AMBR_LOGGER.log : INFO : pid=7527 : Installing
patch(es): 7.3.0U001",
ReceptionTime="2025-07-11 11:04:26",
SenderType="Third Party Device",
EventId="3495"
```

FPT_TUD_EXT.1

FPT_TUD_EXT.1

Failed SMC
Appliance update

```
Timestamp="2025-07-09 11:37:48",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 9 11:37:48 cc-smca AMBR_LOGGER.log : ERROR : pid=17801 : sap
signature file /var/tmp/tmpf8kpzemo/6.11.0U001-unsigned.sap.sig does not
exist.",
ReceptionTime="2025-07-09 11:37:48",
SenderType="Third Party Device",
EventId="4378"
```

```
Timestamp="2025-07-09 11:37:48",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 9 11:37:48 cc-smca AMBR_LOGGER.log : ERROR : pid=17801 : sap
signature file /var/tmp/tmpf8kpzemo/6.11.0U001-unsigned.sap.sig does not
exist.#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 240 in verify_package#012 File 'build/lib/ambr/common/
crypto.py' line 347 in verify_package20#012ValueError: sap signature file /var/
tmp/tmpf8kpzemo/6.11.0U001-unsigned.sap.sig does not exist.",
ReceptionTime="2025-07-09 11:37:48",
SenderType="Third Party Device",
EventId="4379"
```

```
Timestamp="2025-07-09 11:37:48",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 9 11:37:48 cc-smca AMBR_LOGGER.log : ERROR : pid=17801 : Failed to
load: /usr/local/forcepoint/smc/6.11.0U001-unsigned.sap",
ReceptionTime="2025-07-09 11:37:48",
SenderType="Third Party Device",
EventId="4380"
```

```
Timestamp="2025-07-09 11:37:49",
NodeId="192.0.2.22",
CompId="cc-smca-mgmt",
InfoMsg="ERROR: sap signature file /var/tmp/tmpf8kpzemo/6.11.0U001-
unsigned.sap.sig does not exist.ERROR: Unable to load /usr/local/forcepoint/
smc/6.11.0U001-unsigned.sap to /var/ambr/downloaded.ERROR: sap signature file /
var/tmp/tmpf8kpzemo/6.11.0U001-unsigned.sap.sig does not exist.ERROR: Failed to
load: /usr/local/forcepoint/smc/6.11.0U001-unsigned.sap",
SenderType="Management Server",
EventId="7625591619458170995",
UserOriginator="radmin",
ClientIpAddress="192.168.200.10",
TypeDescription="stonegate.mgtserver.appliance_patch.import",
Result="Fail",
ObjectName="SMC Appliance Patch 6.11.0U001-unsigned.sap"
```

```
Timestamp="2025-07-10 08:28:54",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Jul 10 08:28:54 cc-smca AMBR_LOGGER.log : ERROR : pid=27616 : Unable to
get issuer certificate for 'C=US ST=TX O=Forcepoint OU=NGFW CN=NGFW Updates
2020'#012Traceback (most recent call last):#012 File 'build/lib/ambr/common/
crypto.py' line 195 in verify_signer#012 File 'build/lib/ambr/common/crypto.py'
line 140 in verify_chain#012ValueError: Unable to get issuer certificate for
'C=US ST=TX O=Forcepoint OU=NGFW CN=NGFW Updates 2020'",
ReceptionTime="2025-07-10 08:28:54",
SenderType="Third Party Device",
EventId="5111"
```

```
Timestamp="2025-07-10 08:28:54",
NodeId="127.0.0.1",
```

FPT_TUD_EXT.1	
Verification of image (Security Engine)	<pre>Timestamp="2025-04-09 13:26:09", LogId="1245563", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="cc-ngfw-1 node 1", InfoMsg="Engine upgrade: Engine image signature verified", ReceptionTime="2025-04-09 13:26:09", SenderType="Firewall", SituationId="40015", Situation="System_Engine_Upgrade-Succeeded", EventId="7315726719943639419"</pre>
Initiation of Security Engine Engine update	<pre>Timestamp="2025-04-09 13:25:30", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Image sg_engine_7.3.0.31049_x86-64-small.zip", SenderType="Management Server", EventId="8926881974736512916", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.engine.upgrade.start", Result="Success", ObjectName="cc-ngfw-1 node 1"</pre>
Result of the Security Engine Engine update attempt	<pre>Timestamp="2025-04-09 13:27:39", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Image StoneGate firewall(x86-64-small) version 7.3 #31049", SenderType="Management Server", EventId="8926881974736512926", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.engine.upgrade.end", Result="Success", ObjectName="cc-ngfw-1 node 1"</pre>
Failed Security Engine Engine update	<pre>Timestamp="2025-04-14 13:45:05", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Signature verification failed for the Update Package or Engine Upgrade Trust anchor for certification path not found.", SenderType="Management Server", EventId="2695119513275340574", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.mgtserver.upgrade.import", Result="Fail", ObjectName="Engine Upgrade sg_engine_6.11.0.27009.invalid.1_x86-64-small.zip"</pre>
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	<pre>Timestamp="2025-04-07 13:39:28", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Management Client window closed due to idle timeout.", SenderType="Management Server", EventId="1183832478725439491", UserOriginator="radmin", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.session.terminated", Result="Success", ObjectName="radmin"</pre> <pre>Timestamp="2025-04-07 13:39:28", NodeId="192.0.2.2", CompId="cc-smca-mgmt", InfoMsg="Logout succeeded for user radmin.", SenderType="Management Server", EventId="8926881974736507459", UserOriginator="System", ClientIpAddress="192.168.200.1", TypeDescription="stonegate.admin.logout", Result="Success", ObjectName="radmin"</pre>
FTA_SSL.4	
Auditable event	The termination of an interactive session
Termination of local administrative session	<pre>Timestamp="2025-04-04 14:06:56", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Apr 4 14:06:56 cc-smca login: pam_unix(login:session): session closed for user radmin", ReceptionTime="2025-04-04 14:06:56", SenderType="Third Party Device", EventId="6132"</pre>
Termination of remote administrative session	<pre>Timestamp="2025-03-17 16:53:03", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Logout succeeded for user test00.", SenderType="Management Server", EventId="2665307750136807783", UserOriginator="System", ClientIpAddress="127.0.0.1", TypeDescription="stonegate.admin.logout", Result="Success", ObjectName="test00"</pre>
FTA_SSL_EXT.1	
Auditable event	Local session termination

FTA_SSL_EXT.1

Local session termination

```
Timestamp="2025-04-04 14:06:56",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Apr 4 14:06:56 cc-smca audisp-syslog: type=CRED_DISP
msg=audit(1743775616.013:715): pid=75528 uid=0 auid=1000 ses=8
subj=system_u:system_r:local_login_t:s0-s0:c0.c1023 msg='op=PAM:setcred
grantors=pam_unix pam_securetty acct='radmin' exe='/usr/bin/login' hostname=cc-
smca addr=? terminal=/dev/tty1 res=success' UID='root' AUID='radmin'",
ReceptionTime="2025-04-04 14:06:56",
SenderType="Third Party Device",
EventId="6131"
```

```
Timestamp="2025-04-04 14:06:56",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Apr 4 14:06:56 cc-smca login: pam_unix(login:session): session closed
for user radmin",
ReceptionTime="2025-04-04 14:06:56",
SenderType="Third Party Device",
EventId="6132"
```

```
Timestamp="2025-04-04 14:06:56",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Apr 4 14:06:56 cc-smca audisp-syslog: type=SYSCALL
msg=audit(1743775616.013:716): arch=c000003e syscall=188 success=yes
exit=0 a0=562f5a18e350 a1=7fb6549ba1c5 a2=562f5a1b22a0 a3=22 items=1
ppid=1 pid=75528 auid=1000 uid=0 gid=498 euid=0 suid=0 fsuid=0 egid=498
sgid=498 fsgid=498 tty=(none) ses=8 comm='login' exe='/usr/bin/login'
subj=system_u:system_r:local_login_t:s0-s0:c0.c1023 key='perm_mod'
ARCH=x86_64 SYSCALL=setxattr AUID='radmin' UID='root' GID='smca_admin'
EUID='root' SUID='root' FSUID='root' EGID='smca_admin' SGID='smca_admin'
FSGID='smca_admin'",
ReceptionTime="2025-04-04 14:06:56",
SenderType="Third Party Device",
EventId="6133"
```

```
Timestamp="2025-04-04 14:06:56",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Apr 4 14:06:56 cc-smca audisp-syslog: type=PATH
msg=audit(1743775616.013:716): item=0 name='/dev/tty1'
inode=20 dev=00:05 mode=020620 ouid=1000 ogid=5 rdev=04:01
obj=unconfined_u:object_r:user_tty_device_t:s0 nametype=NORMAL cap_fp=0 cap_fi=0
cap_fe=0 cap_fver=0 cap_frootid=0 OUID='radmin' OGID='tty'",
ReceptionTime="2025-04-04 14:06:56",
SenderType="Third Party Device",
EventId="6135"
```

```
Timestamp="2025-04-04 14:06:56",
NodeId="127.0.0.1",
Type="Notification",
CompId="3",
InfoMsg="Apr 4 14:06:56 cc-smca systemd-logind[1141]: Session 8 logged out.
Waiting for processes to exit.",
ReceptionTime="2025-04-04 14:06:56",
SenderType="Third Party Device",
EventId="6137"
```

FTA_SSL_EXT.1	
Local session termination (continued)	<pre> Timestamp="2025-04-04 14:06:56", NodeId="127.0.0.1", Type="Notification", CompId="3", InfoMsg="Apr 4 14:06:56 cc-smca audisp-syslog: type=USER_END msg=audit(1743775616.015:717): pid=75528 uid=0 auid=1000 ses=8 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='radmin' exe='/usr/bin/login' hostname=cc-smca addr=? terminal=/dev/tty1 res=success' UID='root' AUID='radmin'", ReceptionTime="2025-04-04 14:06:56", SenderType="Third Party Device", EventId="6139" </pre>
FTP_ITC.1	
Auditable event	Trusted channel functions
Initiation of the trusted channel	<pre> Timestamp="2025-03-18 13:37:40", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=49771] Local = [host=192.0.2.2 port=8906]", SenderType="Management Server", EventId="2987302565009424590", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.start", Result="Success" </pre>
Termination of the trusted channel	<pre> Timestamp="2025-03-18 13:37:40", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=49771] Local = [port=8906]", SenderType="Management Server", EventId="2987302565009424593", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.end", Result="Success" </pre>
Auditable event	Failure of the trusted channel functions

FTP_ITC.1	
TLS failure	<pre>Timestamp="2025-03-17 16:57:48", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.2 port=54902] Local = [port=8907] ERROR: Failed to check certificate Details: Certificate Error: The Certificate (subjectDN=CN=LogServer 192.0.2.2 serialNumber=4): Responder's certificate not valid for signing OCSP responses", SenderType="Management Server", EventId="2665307750136807967", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>
Connection failure	<pre>Timestamp="2025-02-14 09:41:55", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Connection failed : Peer = [host=192.0.2.10 port=2055] ERROR: Connection refused: /192.0.2.10:2055", SenderType="Management Server", EventId="274981956821713309", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.connection.failure", Result="Fail"</pre>
FTP_TRP.1/Admin	
Auditable event	Trusted path functions
Initiation of the trusted path	<pre>Timestamp="2025-03-17 16:56:46", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.10 port=2055] Local = [host=192.0.2.2 port=57766]", SenderType="Management Server", EventId="2665307750136807942", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.start", Result="Success"</pre>
Termination of the trusted path	<pre>Timestamp="2025-03-17 16:57:55", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.10 port=2055] Local = [host=192.0.2.2 port=57766]", SenderType="Management Server", EventId="2665307750136807977", UserOriginator="System", ClientIpAddress="192.0.2.10", TypeDescription="stonegate.trusted.connection.end", Result="Success"</pre>

FTP_TRP.1/Admin	
Failure of the trusted path functions	<pre>Timestamp="2025-03-17 16:57:48", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection failed : Protocol = NONE Peer = [host=192.0.2.2 port=54902] Local = [port=8907] ERROR: Failed to check certificate Details: Certificate Error: The Certificate (subjectDN=CN=LogServer 192.0.2.2 serialNumber=4): Responder's certificate not valid for signing OCSP responses", SenderType="Management Server", EventId="2665307750136807967", UserOriginator="System", ClientIpAddress="192.0.2.2", TypeDescription="stonegate.trusted.connection.failure", Result="Fail"</pre>
FTP_TRP.1/Join	
Auditable event	Trusted path functions
SMC registration (Initiation)	<pre>Timestamp="2025-03-17 16:40:00", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection started : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=34548] Local = [host=192.0.2.2 port=3021]", SenderType="Management Server", EventId="2661634002615534055", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.start", Result="Success"</pre>
SMC registration (Termination)	<pre>Timestamp="2025-03-17 16:40:20", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=34548] Local = [port=3021]", SenderType="Management Server", EventId="2661634002615534063", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.end", Result="Success"</pre>

FTP_TRP.1/Join	
SMC registration (Failure)	<pre>Timestamp="2025-03-17 16:50:30", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Aborting certificate polling: Certificate Request does not exist. .", SenderType="Management Server", EventId="2665877378764374180", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.engine.initial.contact", Result="Fail", ObjectName="ngfw node 1"</pre> <pre>Timestamp="2025-03-17 16:50:30", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="TLS Connection ended : Protocol = TLSv1.2 Peer = [host=192.0.2.4 port=59028] Local = [port=3021]", SenderType="Management Server", EventId="2665877378764374181", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.trusted.connection.end", Result="Success"</pre>
Security Engine registration (Initiation)	<pre>Timestamp="2025-03-17 16:49:01", LogId="2002", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="TLS: Connected connection (DNS:ManagementServer 192.0.2.2)", ReceptionTime="2025-03-17 16:49:01", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="7307442849014876114"</pre>
Security Engine registration (Termination)	<pre>Timestamp="2025-03-17 16:49:21", LogId="2030", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="TLS: Connection disconnect (DNS:ManagementServer 192.0.2.2)", ReceptionTime="2025-03-17 16:49:21", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="7307442930619254766"</pre>

FTP_TRP.1/Join	
Security Engine registration (Failure)	<pre>Timestamp="2025-03-17 17:22:56", LogId="1981", NodeId="192.0.2.4", Facility="Management", Type="Error", CompId="ngfw node 1", InfoMsg="no shared cipher", ReceptionTime="2025-03-17 17:22:57", SenderType="Firewall", SituationId="9005", Situation="FW_Communication-Communication-Error", EventId="7307451383114893245"</pre> <pre>Timestamp="2025-03-17 17:22:56", LogId="1982", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="TLS: Couldn't accept TLS connection: -3 (DNS:ManagementServer 192.0.2.2)", ReceptionTime="2025-03-17 17:22:57", SenderType="Firewall", SituationId="78002", Situation="TLS connection state", EventId="7307451383114893246"FCO_CPC_EXT.1</pre>
FCO_CPC_EXT.1	
Auditable event	Enabling and disabling communication between the Security Engine and SMC.
Enabling from the Security Engine	<pre>Timestamp="2025-03-28 12:35:24", LogId="685", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="Connection to Management Server (192.0.2.2) enabled", ReceptionTime="2025-03-28 12:35:42", SenderType="Firewall", EventId="7311365292322456237"</pre> <pre>Timestamp="2025-03-28 12:35:40", LogId="1028", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="Connection to Log Server (192.0.2.2) enabled", ReceptionTime="2025-03-28 12:35:42", SenderType="Firewall", EventId="7311365361041933316"</pre>

FCO_CPC_EXT.1	
Disabling from the Security Engine Engine	<pre>Timestamp="2025-03-27 12:40:08", LogId="2711", NodeId="192.0.2.4", Facility="System Utilities", Type="Error", Event="Notice", CompId="ngfw node 1", InfoMsg="Engine factory reset initiated from SMC",ReceptionTime="2025-03-27 12:40:09", SenderType="Firewall", SituationId="500", Situation="FW_Notice", EventId="7311004094162799255"</pre> <pre>Timestamp="2025-03-27 12:40:08", LogId="2712", NodeId="192.0.2.4", Facility="System Utilities", Type="Error", Event="Notice", CompId="ngfw node 1", InfoMsg="Connection to Management Server 192.0.2.2 and Log Server disabled", ReceptionTime="2025-03-27 12:40:09", SenderType="Firewall", SituationId="500", Situation="FW_Notice", EventId="7311004094162799256"</pre>
Enabling from the SMC	<pre>Timestamp="2025-03-17 16:40:00", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="Initial contact from Engine Node", SenderType="Management Server", EventId="2661634002615534052", UserOriginator="System", ClientIpAddress="192.0.2.4", TypeDescription="stonegate.engine.initial.contact", Result="Success", ObjectName="ngfw node 1"</pre>

FCO_CPC_EXT.1

Disabling from the SMC

```
Timestamp="2025-03-28 11:49:28",
NodeId="192.0.2.2",
CompId="Management Server",
SenderType="Management Server",
EventId="6669633148927607040",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.firewall.Reset Engine to Factory Settings",
Result="Success",
ObjectName="ngfw node 1"
```

```
Timestamp="2025-03-28 11:56:29",
NodeId="192.0.2.2",
CompId="Management Server",
SenderType="Management Server",
EventId="6669633148927607049",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.delete",
Result="Success",
ObjectName="ngfw"
```

```
Timestamp="2025-03-28 11:56:29",
NodeId="192.0.2.2",
CompId="Management Server",
SenderType="Management Server",
EventId="6669633148927607051",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
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**

```
Timestamp="2025-04-07 14:17:13",
LogId="1472",
NodeId="192.0.2.4",
Facility="Packet Filtering",
Type="Notification",
Event="Connection discarded",
Action="Discard",
Protocol="58",
Src="::16",
Dst="FF02::16",
RuleId="46.0",
Srcif="2",
IcmpType="143",
IcmpCode="0",
CompId="ngfw node 1",
ReceptionTime="2025-04-07 14:17:34",
SenderType="Firewall",
SituationId="70019",
Situation="Connection_Discarded",
EventId="7315014794753343491",
Service="IPv6 ICMP/143/0"
```

FCS_IPSEC_EXT.1 IPsec Protocol	
Decisions to BYPASS network packets processed by the TOE	BYPASS <pre> Timestamp="2025-04-07 14:15:53", LogId="1390", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="New connection", Action="Allow", Protocol="6", Src="192.0.2.1", Dst="192.0.2.4", Sport="35476", Dport="22", RuleId="120.0", Srcif="0", CompId="ngfw node 1", ReceptionTime="2025-04-07 14:15:54", SenderType="Firewall", SituationId="70018", Situation="Connection_Allowed", EventId="7315014459745894428", Service="SSH" </pre>
Decisions to PROTECT network packets processed by the TOE	PROTECT <pre> Timestamp="2025-04-07 14:21:21", LogId="1727", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="New connection through VPN", Action="Allow", Protocol="1", Src="10.10.0.1", Dst="203.0.113.6", RuleId="128.0", IcmpType="8", IcmpCode="0", CompId="ngfw node 1", ReceptionTime="2025-04-07 14:21:22", SenderType="Firewall", SituationId="71012", Situation="FW_New-IPsec-VPN-Connection", EventId="7315015834135429164", Service="Echo Request (No Code)" </pre>

FCS_IPSEC_EXT.1 IPsec Protocol**IPsec SAs****Failure to establish an IPsec SA**

```
Timestamp="2025-10-29 18:32:09",
LogId="980",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="IKEv2 SA error: Authentication failed: Remote Traffic Selector mismatch
(80) tunnel ID 1073709058",
ReceptionTime="2025-10-29 18:32:09",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7389368461127844820"
```

```
Timestamp="2025-10-29 18:32:09",
LogId="982",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="IPsec SA error: Authentication failed",
ReceptionTime="2025-10-29 18:32:09",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7389368461127844822"
```

FCS_IPSEC_EXT.1 IPsec Protocol**IPsec SA establishment**

```

Timestamp="2025-04-07 14:21:21",
LogId="1725",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Notification",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="IKEv2 SA responder done Local ngfw@engine.com (email) Remote
styx@forcepoint.com (email) Local auth method: RSA signature Remote auth
method: RSA signature Local signature algorithm: sha256WithRSAEncryption
Remote signature algorithm: sha256WithRSAEncryption lifetime 86400 secs
cipher:aes128-cbc mac:hmac-sha256-128 prf:hmac-sha256 DH group:19",
ReceptionTime="2025-04-07 14:21:21",
SenderType="Firewall",
SituationId="12102",
Situation="IKE-SA-Responder-Done",
EventId="7315015829840463549"

```

```

Timestamp="2025-04-07 14:21:21",
LogId="1726",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Notification",
Src="10.10.0.0",
Dst="203.0.113.0",
CompId="ngfw node 1",
InfoMsg="IPsec SA responder done. Encryption:aes128-cbc mac:hmac-sha2/256.
Negotiation took 2 msecs.",
ReceptionTime="2025-04-07 14:21:21",
SenderType="Firewall",
SituationId="12107",
Situation="IPsec-SA-Responder-Done",
EventId="7315015829840463550"

```

FCS_IPSEC_EXT.1 IPsec Protocol**IPsec SA termination**

```
Timestamp="2025-04-07 14:21:27",
LogId="1728",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Notification",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="IPsec SA deleted",
ReceptionTime="2025-04-07 14:21:28",
SenderType="Firewall",
SituationId="12117",
Situation="IPsec-SA-Deleted",
EventId="7315015859905234624"
```

```
Timestamp="2025-04-07 14:21:37",
LogId="1730",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Notification",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="IKE SA deleted",
ReceptionTime="2025-04-07 14:21:37",
SenderType="Firewall",
SituationId="12116",
Situation="IKE-SA-Deleted",
EventId="7315015898559940290"
```

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****Unsuccessful attempt to validate a peer certificate: No CRL service**

```
Timestamp="2025-03-26 15:11:33",
LogId="2193",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="Validating certificate with subject='C=FI CN=styx-CRLfail-leaf
certificate' failed because certificate with subject='C=FI CN=styx-CRLfail-ic
certificate' is not valid: Reason: (did not find trusted CA CRL was not found
path was not verified)",
ReceptionTime="2025-03-26 15:11:33",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7310679811247048849"
```

```
Timestamp="2025-03-26 15:11:33",
LogId="2194",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
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="2025-03-26 15:11:33",
SenderType="Firewall",
EventId="7310679811247048850"
```

```
Timestamp="2025-03-26 15:11:33",
LogId="2195",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="IKEv2 SA error: Authentication failed",
ReceptionTime="2025-03-26 15:11:33",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7310679811247048851"
```

FIA_X509_EXT.1/Rev X.509 Certificate Validation (VPN)**Unsuccessful attempt to validate a peer certificate: Untrusted root CA**

```

Timestamp="2025-03-26 15:12:39",
LogId="2254",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="Validating certificate with subject='C=FI CN=styx-NoCA-leaf
certificate' failed. Reason: (certificate was not found)",
ReceptionTime="2025-03-26 15:12:39",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7310680090419923150"

```

```

Timestamp="2025-03-26 15:12:39",
LogId="2255",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="Certificate lookup error: certificate was not found",
ReceptionTime="2025-03-26 15:12:39",
SenderType="Firewall",
EventId="7310680090419923151"

```

```

Timestamp="2025-03-26 15:12:39",
LogId="2256",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="IKEv2 SA error: Authentication failed",
ReceptionTime="2025-03-26 15:12:39",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7310680090419923152"

```

FIA_X509_EXT.1/Rev X.509 Certificate Validation (VPN)

Unsuccessful attempt to validate a peer certificate: Certificate revoked by OCSP

```
Timestamp="2025-03-26 15:04:56",
LogId="1630",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Warning",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="OCSP result from http://192.0.2.8:1335 for C=FI CN=styx-OCSP-leaf
certificate: certificate is REVOKED ",
ReceptionTime="2025-03-26 15:04:56",
SenderType="Firewall",
EventId="7310678149094704734"
```

```
Timestamp="2025-03-26 15:04:56",
LogId="1632",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="Validating certificate with subject='N/A' failed. Reason: (certificate
was revoked path was not verified)",
ReceptionTime="2025-03-26 15:04:56",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7310678149094704736"
```

```
Timestamp="2025-03-26 15:04:56",
LogId="1634",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="Certificate lookup errors: certificate was revoked path was not
verified",
ReceptionTime="2025-03-26 15:04:56",
SenderType="Firewall",
EventId="7310678149094704738"
```

```
Timestamp="2025-03-26 15:04:56",
LogId="1635",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="IKEv2 SA error: Authentication failed",
ReceptionTime="2025-03-26 15:04:56",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7310678149094704739"
```

FIA_X509_EXT.1/Rev X.509 Certificate Validation (VPN)**Unsuccessful attempt to validate a peer certificate: Certificate revoked by CRL**

```
Timestamp="2025-03-26 15:06:26",
LogId="1764",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="Validating certificate with subject='C=FI CN=styx-CRL3-leaf
certificate' failed. Reason: (certificate was revoked did not find trusted CA
database method failed path was not verified)",
ReceptionTime="2025-03-26 15:06:26",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7310678522756859620"
```

```
Timestamp="2025-03-26 15:06:26",
LogId="1766",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="Certificate lookup errors: certificate was revoked path was not
verified",
ReceptionTime="2025-03-26 15:06:26",
SenderType="Firewall",
EventId="7310678522756859622"
```

```
Timestamp="2025-03-26 15:06:26",
LogId="1767",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="IKEv2 SA error: Authentication failed",
ReceptionTime="2025-03-26 15:06:26",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7310678522756859623"
```

FIA_X509_EXT.1/Rev X.509 Certificate Validation (VPN)**Unsuccessful attempt to validate a peer certificate: Invalid OCSF signer**

```
Timestamp="2025-03-26 15:09:05",
LogId="1957",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="OCSP lookup failed to http://192.0.2.8:1335 for C=FI CN=styx-OCSP3-leaf
certificate: OCSP server is not authorized (possibly missing id-kp-OCSPSigning
extendedKeyUsage)",
ReceptionTime="2025-03-26 15:09:05",
SenderType="Firewall",
EventId="7310679188476790693"
```

```
Timestamp="2025-03-26 15:09:05",
LogId="1960",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="Validating certificate with subject='C=FI CN=styx-OCSP3-leaf
certificate' failed. Reason: (did not find trusted CA CRL was not found
database method failed path was not verified an OCSP responder in the chain
did not have id-kp-OCSPSigning)",
ReceptionTime="2025-03-26 15:09:05",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7310679188476790696"
```

```
Timestamp="2025-03-26 15:09:05",
LogId="1963",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="IKEv2 SA error: Authentication failed",
ReceptionTime="2025-03-26 15:09:05",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7310679188476790699"
```

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 <pre>Timestamp="2025-03-26 15:03:02", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="certificate_authority element has been created.", SenderType="Management Server", EventId="5975793358491091417", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="strongSwan CA"</pre>
	Configuration of trusted certificate authorities <pre>Timestamp="2025-03-26 14:47:00", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="certificate_authority_ref has been removed: <certificate_authority_ref ref='Internal RSA CA for Gateways 20250320'>/>.", SenderType="Management Server", EventId="5973932190247944371", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="VPN profile for test VPN Certificate Authority element logs"</pre> <pre>Timestamp="2025-03-26 14:47:08", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="certificate_authority_ref has been modified on its attribute: ref (CA for test VPN Certificate Authority element logs -> Internal RSA CA for Gateways 20250320).", SenderType="Management Server", EventId="5973932190247944376", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="VPN profile for test VPN Certificate Authority element logs"</pre>

FIA_X509_EXT.1/Rev X.509 Certificate Validation (VPN)**Removal (deletion) of a trusted certificate authority**

```
Timestamp="2025-03-26 14:47:16",
NodeId="192.0.2.2",
CompId="Management Server",
SenderType="Management Server",
EventId="5973932190247944383",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.cryptographic_key.deleted",
Result="Success",
ObjectName="CA for test VPN Certificate Authority element logs"
```

```
Timestamp="2025-03-26 14:47:16",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="Certificate with subject name CN=VPN Certificate Authority element logs.",
SenderType="Management Server",
EventId="5973932190247944384",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.certificate.delete",
Result="Success",
ObjectName="Certificate <CN=VPN Certificate Authority element logs> (2025-04-25)"
```

```
Timestamp="2025-03-26 14:47:16",
NodeId="192.0.2.2",
CompId="Management Server",
SenderType="Management Server",
EventId="5973932190247944382",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.delete",
Result="Success",
ObjectName="CA for test VPN Certificate Authority element logs"
```

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**

```
Timestamp="2025-03-26 14:47:43",
LogId="810",
NodeId="192.0.2.4",
Facility="Management",
Type="Notification",
CompId="ngfw node 1",
InfoMsg="Private key /data/config/ipsec/priv/request202503260247442051647807924.prv has been created",
ReceptionTime="2025-03-26 14:47:45",
SenderType="Firewall",
SituationId="40010",
Situation="System_Engine-Cryptkeys-Created",
EventId="7310673815472702250"
```

FMT SMF.1/VPN FAU_GEN.1.1 c) All administrative actions (VPN)**Certificate signing request**

```
Timestamp="2025-03-26 14:47:45",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="Certificate Request requested to Engine.",
SenderType="Management Server",
EventId="5973932190247944452",
UserOriginator="System",
ClientIpAddress="192.0.2.2",
TypeDescription="stonegate.vpn.certificate.request",
Result="Success",
ObjectName="ngfw;Certificate Request <CN=Audit External PKI> RSA / SHA-512"
```

```
Timestamp="2025-03-26 14:47:45",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="certificate_request element has been created.",
SenderType="Management Server",
EventId="5973932190247944451",
UserOriginator="System",
ClientIpAddress="192.0.2.2",
TypeDescription="stonegate.object.insert",
Result="Success",
ObjectName="Certificate Request <CN=Audit External PKI> RSA / SHA-512"
```

Import of a signed certificate

```
Timestamp="2025-03-26 14:47:53",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="certificate element has been created.",
SenderType="Management Server",
EventId="5973932190247944453",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.insert",
Result="Success",
ObjectName="Certificate <CN=Audit External PKI> RSA / SHA-256 (2025-04-25)"
```

Configuration of remote VPN client session timeout

```
Timestamp="2025-03-26 14:47:24",
NodeId="192.0.2.2",
CompId="Management Server",
InfoMsg="web_authentication has been modified on its attribute:
authentication_idle_timeout (10000 -> 11111).",
SenderType="Management Server",
EventId="5973932190247944401",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update.details",
Result="Success", ObjectName="ngfw"
```

FMT SMF.1/VPN FAU_GEN.1.1 c) All administrative actions (VPN)**Configuration of the cryptographic functionality****Configuration of IPSec functionality**

```
Timestamp="2025-03-26 14:47:18",
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="5973932190247944392",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="VPN profile for test VPN profile element"
```

```
Timestamp="2025-03-26 14:47:18",
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="5973932190247944390",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="VPN profile for test VPN profile element"
```

```
Timestamp="2025-03-26 14:47:18",
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="5973932190247944389",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="VPN profile for test VPN profile element"
```

```
Timestamp="2025-03-26 14:47:18",
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="5973932190247944391",
UserOriginator="test00",
ClientIpAddress="192.0.2.1",
TypeDescription="stonegate.object.update.details",
Result="Success",
ObjectName="VPN profile for test VPN profile element"
```

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 <pre> Timestamp="2025-03-26 14:47:18", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="sa_life_time has been modified (86400 -> 43200).", SenderType="Management Server", EventId="5973932190247944387", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="VPN profile for test VPN profile element" </pre>
	Configuring IKEv2 Child SA lifetimes <pre> Timestamp="2025-03-26 14:47:18", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="sa_life_time has been modified (86400 -> 43200).", SenderType="Management Server", EventId="5973932190247944387", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="VPN profile for test VPN profile element" </pre>
FPF_RUL_EXT.1 Packet Filtering Rules	
Auditable event	Application of rules configured with the log operation
Application of rules configured with the 'log' operation (VPN)	Drop traffic <pre> Timestamp="2025-04-07 14:17:13", LogId="1472", NodeId="192.0.2.4", Facility="Packet Filtering", Type="Notification", Event="Connection discarded", Action="Discard", Protocol="58", Src="::16", Dst="FF02::16", RuleId="46.0", Srcif="2", IcmpType="143", IcmpCode="0", CompId="ngfw node 1", ReceptionTime="2025-04-07 14:17:34", SenderType="Firewall", SituationId="70019", Situation="Connection_Discarded", EventId="7315014794753343491", Service="IPv6 ICMP/143/0" </pre>

FPF_RUL_EXT.1 Packet Filtering Rules**Permit traffic (BYPASS)**

```
Timestamp="2025-04-07 14:15:53",
LogId="1390",
NodeId="192.0.2.4",
Facility="Packet Filtering",
Type="Notification",
Event="New connection",
Action="Allow",
Protocol="6",
Src="192.0.2.1",
Dst="192.0.2.4",
Sport="35476",
Dport="22",
RuleId="120.0",
Srcif="0",
CompId="ngfw node 1",
ReceptionTime="2025-04-07 14:15:54",
SenderType="Firewall",
SituationId="70018",
Situation="Connection_Allowed",
EventId="7315014459745894428",
Service="SSH"
```

Permit traffic (PROTECT)

```
Timestamp="2025-04-07 14:21:21",
LogId="1727",
NodeId="192.0.2.4",
Facility="Packet Filtering",
Type="Notification",
Event="New connection through VPN",
Action="Allow",
Protocol="1",
Src="10.10.0.1",
Dst="203.0.113.6",
RuleId="128.0",
IcmpType="8",
IcmpCode="0",
CompId="ngfw node 1",
ReceptionTime="2025-04-07 14:21:22",
SenderType="Firewall",
SituationId="71012",
Situation="FW_New-IPsec-VPN-Connection",
EventId="7315015834135429164",
Service="Echo Request (No Code)"
```

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

Auditable event	Trusted channel functions
-----------------	---------------------------

FTP_ITC.1/VPN Inter-TSF Trusted Channel (VPN Communications)	
Initiation of the trusted channel	<pre> Timestamp="2025-04-07 14:21:21", LogId="1725", NodeId="192.0.2.4", Facility="IPsec VPN", Type="Notification", Src="10.0.200.10", Dst="198.51.100.4", Sport="500", Dport="500", CompId="ngfw node 1", InfoMsg="IKEv2 SA responder done Local ngfw@engine.com (email) Remote styx@forcepoint.com (email) Local auth method: RSA signature Remote auth method: RSA signature Local signature algorithm: sha256WithRSAEncryption Remote signature algorithm: sha256WithRSAEncryption lifetime 86400 secs cipher:aes128-cbc mac:hmac-sha256-128 prf:hmac-sha256 DH group:19", ReceptionTime="2025-04-07 14:21:21", SenderType="Firewall", SituationId="12102", Situation="IKE-SA-Responder-Done", EventId="7315015829840463549" </pre>
Termination of the trusted channel	<pre> Timestamp="2025-04-07 14:21:37", LogId="1730", NodeId="192.0.2.4", Facility="IPsec VPN", Type="Notification", Src="10.0.200.10", Dst="198.51.100.4", Sport="500", Dport="500", CompId="ngfw node 1", InfoMsg="IKE SA deleted", ReceptionTime="2025-04-07 14:21:37", SenderType="Firewall", SituationId="12116", Situation="IKE-SA-Deleted", EventId="7315015898559940290" </pre>

FTP_ITC.1/VPN Inter-TSF Trusted Channel (VPN Communications)**Failure of the trusted channel functions**

```
Timestamp="2025-10-24 21:47:09",
LogId="2448",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="No rule found for selectors ipv4(icmp:2048 203.0.113.6)
ipv4(203.0.113.0-203.0.113.255) <-> ipv4(icmp:2048 10.10.0.1)
ipv4(10.10.0.0-10.10.0.255) and for IKE peers 198.51.100.4 and 10.0.200.10 and
IKE IDs local ngfw@engine.com (email) and remote foobar@forcepoint.com (email):
Remote ID mismatch",
ReceptionTime="2025-10-24 21:47:09",
SenderType="Firewall",
EventId="7387605596096170384"
```

```
Timestamp="2025-10-24 21:47:09",
LogId="2449",
NodeId="192.0.2.4",
Facility="IPsec VPN",
Type="Error",
Src="10.0.200.10",
Dst="198.51.100.4",
Sport="500",
Dport="500",
CompId="ngfw node 1",
InfoMsg="IKEv2 SA error: Authentication failed: Remote ID mismatch (200) tunnel
ID 1073709058",
ReceptionTime="2025-10-24 21:47:09",
SenderType="Firewall",
SituationId="12168",
Situation="IKE-Authentication-Failed",
EventId="7387605596096170385"
```

FTA_TSE.1.1 TOE Session Establishment**Auditable event**

FTA_TSE.1.1 TOE Session Establishment	
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day)	Configuration of attributes used to deny establishment of remote VPN client session (time, day) <pre> Timestamp="2025-03-26 14:47:31", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="rule_entry (@123.0) has been added: <rule_entry name='discard ISAKMP and NAT-T' is_disabled='false' parent_rule_ref='Access rule : insert point' rank='-25.0' rule_tag_major_id='123' tag='123.0'><match_part><match_sources><match_source_ref type='network_element' value='ANY'/></match_sources><match_destinations><match_destination_ref type='network_element' value='\$\$ Local Cluster'/></match_destinations><match_service_ref type='application' value='ISAKMP'/><match_service_ref type='application' value='NAT-T'/></match_services><rule_validity_times><rule_validity_time_ref type='rule_validity_time' value='Weekends'/></rule_validity_times></match_part><option><log_policy closing_mode='true' log_level='undefined' mss_enforce='false'><payload_modes><payload_mode type='string' value='nothing'/></payload_modes></log_policy></option></ rule_entry>.", SenderType="Management Server", EventId="5973932190247944426", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="auditpolicy" </pre>
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	<pre> Timestamp="2025-03-26 14:47:28", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="rule_validity_time element has been created.", SenderType="Management Server", EventId="5973932190247944417", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.insert", Result="Success", ObjectName="Weekends" </pre>
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	<pre> Timestamp="2025-03-26 14:47:40", 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="5973932190247944437", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Weekends" </pre>

FTA_TSE.1.1 TOE Session Establishment	
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	<pre>Timestamp="2025-03-26 14:47:40", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="rule_time_repeat_end has been modified (07:00 -> 06:00).", SenderType="Management Server", EventId="5973932190247944438", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="Weekends"</pre>
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	<pre>Timestamp="2025-03-26 14:47:40", NodeId="192.0.2.2", RuleId="124.1", CompId="Management Server", InfoMsg="IPv4 Access @124.1 has been modified.", SenderType="Management Server", EventId="5973932190247944441", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="auditpolicy"</pre>
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	<pre>Timestamp="2025-03-26 14:47:40", NodeId="192.0.2.2", CompId="Management Server", InfoMsg="rule_validity_times has been added: <rule_validity_times><rule_validity_time_ref type='rule_validity_time' value='Weekends' /></rule_validity_times>.", SenderType="Management Server", EventId="5973932190247944442", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update.details", Result="Success", ObjectName="auditpolicy"</pre>
Configuration of attributes used to deny establishment of remote VPN client session (location, time, day) (Continued)	<pre>Timestamp="2025-03-26 14:47:40", NodeId="192.0.2.2", CompId="Management Server", SenderType="Management Server", EventId="5973932190247944443", UserOriginator="test00", ClientIpAddress="192.0.2.1", TypeDescription="stonegate.object.update", Result="Success", ObjectName="auditpolicy"</pre>
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)	<pre> Timestamp="2025-03-27 16:44:32", LogId="1107", NodeId="192.0.2.4", Facility="System Utilities", Type="Notification", CompId="ngfw node 1", InfoMsg="Thu Mar 27 16:43:48 UTC 2025 SHA512withECDSA checksum of the root file system succeed", ReceptionTime="2025-03-27 16:44:33", SenderType="Firewall", SituationId="73200", Situation="Self_Test-Success", EventId="7311065602389443667" </pre> <pre> Timestamp="2025-03-27 16:44:32", LogId="1102",NodeId="192.0.2.4", Facility="System Utilities", Type="Notification", CompId="ngfw node 1", InfoMsg="Thu Mar 27 16:43:31 UTC 2025 Cryptographic self-tests succeeded", ReceptionTime="2025-03-27 16:44:33", SenderType="Firewall", SituationId="73202", Situation="Self_Test-Cryptography-Success", EventId="7311065602389443662" </pre> <pre> Timestamp="2025-03-27 16:44:32", LogId="1120", NodeId="192.0.2.4", Facility="Management", Type="Notification", CompId="ngfw node 1", InfoMsg="Thu Mar 27 16:43:48 2025 Integrity check: Engine image signature verified", ReceptionTime="2025-03-27 16:44:33", SenderType="Firewall", SituationId="73200", Situation="Self_Test-Success", EventId="7311065602389443680" </pre>
Indication that TSF self-test was completed (SMC)	<pre> Timestamp="2025-03-26 14:46:50", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Mar 26 14:46:50 smca-mn-xray sudo: test00 : PWD=/home/test00 ; USER=root ; COMMAND=/bin/grep 'smca-mn-xray root: fipscheck:Performing FIPS integrity check\\.\.\.\.\\$' /var/log/smca/smca.log", ReceptionTime="2025-03-26 14:46:50", SenderType="Third Party Device", EventId="3371" </pre>

FAU_GEN.1/VPN Audit Data Generation (VPN Gateway)	
Failure of self-test (NGFW)	<pre>Timestamp="2025-04-07 14:17:47", LogId="1", NodeId="192.0.2.4", Facility="System Utilities", Type="System alert", CompId="ngfw node 1", InfoMsg="Mon Apr 7 14:16:01 UTC 2025 SHA512withECDSA checksum of the root file system failed", ReceptionTime="2025-04-07 14:17:48", SenderType="Firewall", SituationId="73201", Situation="Self_Test-Fail", AlertSeverity="Critical", EventId="7315014936755699713"</pre> <pre>Timestamp="2025-04-07 14:17:47", LogId="1571", NodeId="192.0.2.4", Facility="System Utilities", Type="System alert", CompId="ngfw node 1", InfoMsg="Mon Apr 7 14:16:01 UTC 2025 FIPS: rootfs integrity check FAILED rebooting...", ReceptionTime="2025-04-07 14:27:05", SenderType="Firewall", SituationId="73201", Situation="Self_Test-Fail", EventId="7315014936487265827"</pre>
Failure of self-test (SMC)	<pre>Timestamp="2025-04-07 14:26:59", NodeId="::1", Type="Notification", CompId="3", InfoMsg="Apr 7 14:26:02 smca-mn-xray root: Fatal FIPS Error: fipscheck:ERROR:FIPS integrity check failed. /usr/bin/smca-fipscheck: 255", ReceptionTime="2025-04-07 14:26:59", SenderType="Third Party Device", EventId="2340"</pre>

Secure the update process

When applying appliance upgrades and patches, review and follow the guidance in the *Forcepoint Network Security Platform Product Guide* to ensure that the update is secure.



Note

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

For more information, see the *SMC Appliance maintenance* chapter and the *Upgrading Security Engines* chapter in the *Forcepoint Network Security Platform Product Guide*.

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

SMC Appliance and Security 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 Security Engine updates, the SMC verifies the Security Engine update signature when the update is imported to the SMC. Only valid updates can be imported and installed on the Security 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 **Administration > Engine Upgrades**.
 - Remove the unnecessary imported Engine Upgrades. To remove the upgrade, right-click the upgrade and select the **Delete** option.
 - Select **Administration > SMC Appliance Patches**.
 - Remove the unnecessary imported SMC Appliance Patches. To remove the patch, right-click the patch and select the **Unload** option.
 - Try to import the update again.

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

If an incorrect Security Engine version update was applied, you can revert to the previous installed Security 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:

Steps

- 1) Download the SMC Appliance patch file (7.3.2U001.sap, for example) from <https://support.forcepoint.com/s/download>.
- 2) To patch or upgrade the SMC Appliance, see the *Patch or upgrade the SMC Appliance on the command line* topic in the *Forcepoint Network Security Platform Installation Guide*.

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 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 Engine 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 SMC Client or using SMC Web Access.
- 2) Right-click the Engine related to the **VPN problem** on the **Home / Dashboard** page, and then select **Monitoring > Logs by Sender**.



Note

If the VPN is failing between two 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 Engine 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 Engine 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 Engine will be the responder, and thus more detailed error should be seen in the Engine 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 Engine 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 Network Security Platform 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.

Process	Listening	Ports/Protocol	Contacting	Hardware Privilege	User	Linux Capabilities	TLS	Description
/usr/local/forcepoint/smc/jre/bin/java	Log Server	3020/TCP	Security Engines	Ring 3	sgadmin	0	Server	Log and alert messages; monitoring of blacklists, connections, status, and statistics from Security Engine Engines.
/usr/local/forcepoint/smc/jre/bin/java	Log Server	8914-8918/TCP	SMC Client	Ring 3	sgadmin	0	Server	Log browsing.
/usr/local/forcepoint/smc/jre/bin/java	Management Server	3021/TCP	Log Server, Security 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	SMC Client, Log Server	Ring 3	sgadmin	0	Server	Monitoring and control connections.
/usr/local/forcepoint/smc/jre/bin/java	Management Server	8906/TCP	Security Engines	Ring 3	sgadmin	0	Server	Monitoring and control connections.
/usr/local/forcepoint/smc/jre/bin/java	Management Server	3023/TCP	Log Server, Security 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	0xffffffffffff=all	No	Requesting health and other information about the SMC Appliance.
/usr/local/forcepoint/smc/jre/bin/java	Syslog server	6514/TCP	Management Server, Log Server	Ring 3	sgadmin	0	Client	Audit and log data forwarding to syslog servers.
/usr/sbin/snmpd	Third-party components	162/UDP	SMC Appliance	Ring 3	snmp	0xffffffffffff=all	No	Sending SNMP status probing to external devices.

Process	Listening	Ports/ Protocol	Contact-ing	Hardware Privilege	User	Linux Capabilities	TLS	Description
/usr/local/forcepoint/smc/jre/bin/java	Update servers	443/TCP	Management Server	Ring 3	sgadmin	0	Client	Update packages, Security Engine Engine upgrades, and licenses.
/usr/bin/python	Update servers	443/TCP	SMC Appliance	Ring 3	root	0xffffffffffff=all	Client	Receiving appliance patches and updates.

Processes for Security Engines

Process	Listening	Ports/ Protocol	Contact-ing	Hardware Privilege	User	Linux Capabilities	TLS	Description
/usr/sbin/slapd_proxy	Firewall	636/TCP	Management Server	Ring 3	sgadmin	0x0000003fffffff	Server	Internal user database replication.
/usr/sbin/authd	Firewall	2543/TCP	Any	Ring 3	root	0x0000003fffffff	No	User authentication (Telnet) for Access rules. Denied by default.
/usr/sbin/upgrd	Firewall	4950/TCP	Management Server	Ring 3	root	0x0000003fffffff	Server	Remote upgrade.
/usr/sbin/mgmttd	Firewall	4987/TCP	Management Server	Ring 3	root	0x0000003fffffff	Server	Management Server commands and policy upload.
/usr/sbin/blocklistd	Firewall	15000/TCP	Management Server	Ring 3	root	0x0000003fffffff	Server	Block list entries.
/usr/sbin/smonitd	Firewall	161/UDP	SNMP server	Ring 3	smonitd	0x0000003fffffff	No	SNMP monitoring.
/usr/sbin/sendlogd	Log Server	3020/TCP	Engine	Ring 3	root	0x0000003fffffff	Client	Log and alert messages; monitoring of blacklists, connections, status, and statistics.
/usr/lib/stonegate/bin/contact	Management Server	3021/TCP	Engine	Ring 3	root	0x0000003fffffff	Client	System communications certificate request/renewal (initial contact).
/usr/sbin/sendlogd	Management Server	3023/TCP	Engine	Ring 3	root	0x0000003fffffff	Client	Monitoring (status) connection.

Process	Listening	Ports/ Protocol	Contact- ing	Hardware Privilege	User	Linux Capabilities	TLS	Description
/usr/sbin/ smonitd	SNMP server	162/UDP	Engine	Ring 3	smonitd	0x0000003fffffffff	No	SNMP traps from the Security Engine Engine.
/usr/sbin/ dnsmasq	Firewall	53/TCP, 53/UDP	Any	Ring 3	nobody	0x0000003fffffffff	No	DNS relay

