Network Security Platform

7.3.1

Security Engine

Release Notes

Revision A

Contents

About this release

This document contains important information about this release of the Security Engine of the Forcepoint Network Security Platform. We strongly recommend that you read the entire document.

Product name change

Starting from Forcepoint Network Security Platform version 7.3 release the product name has changed from Forcepoint FlexEdge Secure SD-WAN to Forcepoint Network Security Platform. The primary changes are listed below:

Component	Old name	New name
Solution	Forcepoint FlexEdge Secure SD-WAN	Forcepoint Network Security Platform
Management	FlexEdge Secure SD-WAN Manager / SD-WAN Manager Console (SMC)	Security Management Center (SMC)
Engine	FlexEdge Secure SD-WAN Engine	Security Engine

Currently, product name change is visible in SMC and in the following documentations:

- *Forcepoint Security Management Center API User Guide*
- *Forcepoint Network Security Platform Installation Guide*
- *Forcepoint Network Security Platform Product Guide*
- *Forcepoint Network Security Platform Online Help*
- *Forcepoint Network Security Platform Quick Start Guide*

For more information on SMC UI terminology change, refer to the **About this Help** section in the *Forcepoint Network Security Platform Product Guide*.

Note

Some documentations, knowledge base articles, and other support information are still using the old product name.

Experimental Features

Some features are marked as *Experimental*. These are newly introduced features or enhancements that are still in the testing phase and may not yet be fully polished or stable. They are released to gather user feedback and identify potential issues before a broader rollout.

Lifecycle model

This release of Forcepoint Network Security Platform's Security Management Center is a Long-Term Support (LTS) version.

We recommend using the most recent Long-Term Support (LTS) maintenance versions if you do not need any features from a Feature Stream version.

For more information about the Forcepoint Network Security Platform lifecycle policy, see https://support.forcepoint.com/ProductSupportLifeCycle.

System requirements

To use this product, your system must meet these basic hardware and software requirements.

Security Engine appliances

We strongly recommend using a pre-installed Security Engine appliance for Forcepoint Network Security Platform installations.

Note

Some features are not available for all appliance models. See Knowledge Base article 9743 for appliance-specific software compatibility information.

The majority of the following supported appliances can be used in the Security Engine with Layer 3 Interfaces, or Security Engine with Layer 2 Interfaces.

- 60 Series (60, 60L, and 61)
- 120 Series (120, 120L, 120W, 120WL, and 125L)
- 130 Series
- 330 Series (330, 331, and 335)
- 350 Series (352 and 355)

- 1100 Series (1101 and 1105)
- 1202
- 2100 Series (2101 and 2105)
- 2200 Series (2201, 2205, and 2210)
- 2300 Series (2301, 2305, and 2310)
- 3300 Series (3301 and 3305)
- 3400 Series (3401, 3405, and 3410)
- 3500 Series (3505 and 3510)
- 6205

Basic hardware requirements

You can install Security Engine on standard hardware with these basic requirements.

Component	Requirement
CPU	Intel® processors based on Westmere (microarchitecture) or newer.
Memory	Minimum 4 GB of RAM
Hard disk	Minimum 8 GB **Note** RAID controllers are not supported.
Peripherals	■ DVD drive / External USB storage ■ VGA-compatible display ■ Keyboard
Interfaces	■ One or more network interfaces for the Security Engine with Layer 3 Interfaces ■ Two or more network interfaces for the IPS in IDS configuration ■ Three or more network interfaces for inline Engines with Layer 2 Interfaces for IPS or Layer 2 Engine deployment For information about supported Ethernet interface types and adapters, see Knowledge Base article 9721.

Master Engine requirements

Master Engines have specific hardware requirements.

- Each Master Engine must run on a separate physical device. For more details, see the *Forcepoint Network Security Platform Installation Guide*.
- All Virtual Engines hosted by a Master Security Engine or Master Security Engine cluster must have the same role and the same Failure Mode (*fail-open* or *fail-close*).

- Master Security Engines can allocate VLANs or interfaces to Virtual Security Engines. If the Failure Mode of the Virtual IPS engines or Virtual Layer 2 Engines is *Normal* (fail-close) and you want to allocate VLANs to several Security Engines, you must use the Master Security Engine cluster in standby mode.
- Cabling requirements for Master Security Engine clusters that host Virtual IPS engines or Layer 2 Engines:
  - Failure Mode *Bypass* (fail-open) requires IPS serial cluster cabling.
  - Failure Mode *Normal* (fail-close) requires Layer 2 Engine cluster cabling.

  For more information about cabling, see the *Forcepoint Network Security Platform Installation Guide*.

Virtual appliance node requirements

You can install Security Engine on virtual appliances with these hardware requirements. Also be aware of some limitations.

Component	Requirement
CPU	Intel® processors based on Westmere microarchitecture or newer.
Memory	Minimum 4 GB of RAM
Virtual disk space	Minimum 8 GB
Hypervisor	One of the following: - VMware ESXi 7.0 or 8.0 - KVM with Red Hat Enterprise Linux 8.5 or 9.x - (Engine with Layer 3 Interfaces only) Microsoft Hyper-V on Windows Server 2016 with an Intel 64-bit processor
Interfaces	- At least one virtual network interface for the Security Engine with Layer 3 Interfaces - Three virtual network interfaces for Engines with Layer 2 Interfaces The following network interface card drivers are recommended: - VMware ESXi platform — `vmxnet3`. - KVM platform — `virtio_net`.

When Security Engine is run as a virtual appliance node, these limitations apply:

- Only Packet Dispatching CVI mode is supported.
- Only standby clustering mode is supported.
- Heartbeat requires a dedicated non-VLAN-tagged interface.

When Security Engine is run as a virtual appliance node in the Engines with Layer 2 Interfaces, clustering is not supported.

Supported cloud environments

You can deploy the Security Engine in Amazon Web Services (AWS), Microsoft Azure, and other public cloud environments supported by Google, IBM, and Oracle.

For more information about deploying the Security Engine:

1) In AWS, see the document *How to deploy Forcepoint Network Security Platform in the Amazon Web Services cloud* and Knowledge Base article 10156.

2) In Microsoft Azure, see the document *How to deploy Forcepoint Network Security Platform in the Azure cloud* and Knowledge Base article 14485.

3) In other cloud environments, see the Knowledge Base article 39116.

Important

a) For AWS and Microsoft Azure, Security Engine instances can be launched using 1-Click Launch and custom solution templates, respectively. Existing instances can be remotely upgraded to the latest Security Engine version.

b) For other cloud environments, the Security Engine deliverables include a qcow2 formatted virtual machine disk image, which facilitates easier deployment to cloud platforms supported by Google, IBM, and Oracle.

Build number and checksums

The build number for Security Engine 7.3.1 is 31106.

Use the checksums to make sure that the installation files downloaded correctly.

- sg_engine_7.3.1.31106_x86-64-small.iso

```
SHA256SUM:
c9b73e0fc2a4dbbe651c1279d8f38d1f28a36da600668648dd679634add222ff

SHA512SUM:
767c9323f2a7153c10b6d21a3402e628
6055057a1e70ed08084d0bc5a0b2f3a3
78475b0ddb39cd9c00e0f5de894ebb45
26496c2eccce717ea8b2e8acad05be53
```

- sg_engine_7.3.1.31106_x86-64-small.zip

```
SHA256SUM:
08981108ac1ea9310a96b0aa9fc99b56dcd9b5cae6a4205d36b4dfdb296576e9

SHA512SUM:
2d7c09bc0ab3889638c70a21cdbbd589
793e4b508044592781c1c7e85a1bc497
ccf05a5c7ceba5ad3b19d214d330f565
bfcd8226d24c2830cebfe40da73e3034
```

- Forcepoint-NGFW-gencloud-7.3.1.31106.qcow2

```
SHA256SUM
a5a817da9763cd71aea05bfda8552d2b8cdc41174a19d53694aef483a8607743

SHA512SUM
e6650507b38e4252ccb6f4265adfe252
5d0bc2b3fa831fd0ff7bdd69ab4c0bc1
76b1a73d7392d167339e900c2c9a11c6
838dac9da1ca223c33cff9e2f0242af5
```

Compatibility

Security Engine 7.3 is compatible with the following component versions.

- Forcepoint Security Management Center 7.3 or higher
- Dynamic Update 1841 or higher
- Forcepoint VPN Client 6.6.0 or higher for Windows
- Forcepoint VPN Client 2.0.0 or higher for Mac OS X
- Forcepoint VPN Client 2.0.0 or higher for Android
- Forcepoint VPN Client 2.5.0 or higher for Linux
- Server Pool Monitoring Agent 4.0.0 or higher
- Forcepoint Endpoint Context Agent (ECA) included in Forcepoint One Endpoint 19.05 or higher
- Forcepoint User ID Service 2.0.0 or higher

New features

This release of the product includes these new features. For more information and configuration instructions, see the *Forcepoint Network Security Platform Product Guide*, the *Forcepoint Network Security Platform Installation Guide*, and the *Forcepoint NGFW Manager and VPN Broker Product Guide*.

Post-quantum Pre-shared Key

Post-quantum security is now supported for site-to-site IPsec VPN tunnels by mixing preshared keys within the Internet Key Exchange Protocol Version 2 (IKEv2) as specified in RFC 8784.

Explicit proxy support for HTTP and HTTPS protocols (Experimental)

The Security Engine can be configured to act as an explicit proxy for HTTP and HTTPS connections. Proxy authentication is supported. This feature's support status is experimental in this release.

Enhancements

This release of the product includes these enhancements.

Enhancements in Security Engine version 7.3.1

Enhancement	Description
Log Server per Virtual Engine	You can now assign a dedicated log server to a virtual engine. Previously, the log data from virtual engine was sent to the same log server as the master engine.

Enhancements in Security Engine version 7.3.0

Enhancement	Description
AES-GCM-256 support in IKEv2	IPsec VPNs can now be configured to use AES-GCM cipher mode also in IKE negotiations. This mode is used in three new predefined VPN profiles: CNSA-GCM-256-ECDH-384, CNSA-GCM-256-DH-3072 and CNSA-GCM-256-DH-4096.
Wi-Fi 6 (802.11ax) support	WLAN interface configuration now supports new 802.11ax wireless mode and WPA3 security that can be used with compatible appliance revisions.
CRL prefetching	Administrator configured certificate revocation lists (CRLs) can now be fetched and cached even before those are needed for certificate validation.
Dynamic routing suite upgrade	FRRouting protocol suite for dynamic routing support has been upgraded to 9.1 version.
Security Engine kernel update	Security Engine has been updated to 6.6 version.
Security Engine OS updates	■ Security Engine operating system has been refreshed to a newer version ■ FIPS mode utilizes FIPS 140-3 cryptographic modules: ■ #4835 for IPsec ■ #4898 for IKE ■ #4985 for TLS and other purposes
SHA-256 and AES-256 algorithms support added for SNMPv3 agent	SNMPv3 agent has been enhanced to support SHA-256 and AES-256 algorithms.
SNMP trap from disconnected log server	When SNMP Agent is configured for Security Engine and Hardware Alerts SNMP trap is activated, Security Engine now sends an SNMP trap with MIB OID `forcepointNGFWEngineMib.engineObjects.netNodeObjects.nodeHwmonEvent` if the log server connection has been unavailable for more than 5 minutes.
Extending Layer 2 networks across Layer 3 boundaries (Experimental)	Security Engine with Layer 2 Interfaces using VXLAN (Virtual Extensible LAN) and VTEP (Virtual Tunnel End Point) provides a solution for extending Layer 2 Interfaces across Layer 3 boundaries. For detailed instructions, see Knowledge Base article 11858.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 11660.

Security updates

For information about third-party packages and associated vulnerabilities included with the Security Engine in this product release, see Knowledge Base article 11725 .

Installation instructions

Use these high-level steps to install the SMC and the Security Engines.

For detailed information, see the *Forcepoint Network Security Platform Installation Guide*. All guides are available at help.forcepoint.com.

Steps

1) Install the Management Server, the Log Servers.

2) Import the licenses for all components.
   You can generate licenses at https://stonesoftlicenses.forcepoint.com.

3) Configure the Engine elements in the SMC Client from the **Engine Configuration** navigation menu.

4) To generate initial configurations, right-click each Security Engine, then select **Configuration** > **Save Initial Configuration**.
   Make a note of the one-time password.

5) Make the initial connection from the Security Engines to the Management Server, then enter the one-time password.

6) Create and upload a policy on the Security Engines in the SMC Client.

Upgrade instructions

Take the following into consideration before upgrading licenses, Security Engines, and clusters.

Note

Upgrading to version 7.3 is only supported from version 7.1 or higher. If you have a lower version, first upgrade to version 7.1.

- Forcepoint Network Security Platform version 7.3 requires an updated license. The license upgrade can be requested at https://stonesoftlicenses.forcepoint.com. Install the new license using the SMC Client before upgrading the software. If communication between the SMC and the license server is enabled and the maintenance contract is valid, the license is updated automatically.
- To upgrade the Security Engine, use the remote upgrade feature or reboot from the installation DVD and follow the instructions. For detailed instructions, see the *Forcepoint Network Security Platform Installation Guide*.

Deprecated features

Before upgrading, please consider these feature deprecations.

Feature	Description
Legacy IPsec VPN algorithms removed	Support for legacy and insecure IPsec VPN algorithms has been removed. This includes the removal of support for DES and Blowfish ciphers, the MD5 message digest algorithm, and Diffie-Hellman groups 1 (768 bit) and 2 (1024 bit).

Find product documentation

In the Forcepoint Customer Hub, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product in the Forcepoint Customer Hub at https://support.forcepoint.com. There, you can access product documentation, release notes, Knowledge Base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint Customer Hub. If you do not yet have credentials, create a customer account. To create a customer account, navigate to the Customer Hub Home page, and then click the **Create Account** link.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint Network Security Platform Product Guide*
- *Forcepoint Network Security Platform Online Help*

Note

By default, the Online Help is used from the Forcepoint help server. If you want to use the online Help from a local machine (for example, an intranet server or your own computer), see Knowledge Base article 10097.

- *Forcepoint Network Security Platform Installation Guide*

Other available documents include:

- *Forcepoint Hardware Guide* for your model
- *Forcepoint Network Security Platform Quick Start Guide*

- *Forcepoint Security Management Center API User Guide*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*
- *Forcepoint NGFW Manager and VPN Broker Product Guide*

Published 20 November 2025