Forcepoint

Network Security Platform

7.5.0

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.

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 Security Management Center is a Feature Stream (FS) version.

Support for Feature Stream versions is discontinued when a new major version of Forcepoint Network Security Platform is available.

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 (130 and 130WL)
- 330 Series (330 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)
- 3400 Series (3401, 3405, and 3410)
- 3500 Series (3505 and 3510)

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.

Component	Requirement
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 9.x or 10.x ■ (Engine with Layer 3 Interfaces only) Microsoft Hyper-V on Windows Server 2016 with an Intel 64-bit processor

Component	Requirement
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 7.5.0 is 33034.

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

- sg_engine_7.5.0.33034_x86-64-small.iso

```
SHA256SUM:
4e9834dda44c2dd6f3e9427a4d177ab1af5b220143bd495c51cedea914f5ff77

SHA512SUM:
bf086b3c90aa7da1101db5386e75cf75
50cfa16a2a331978ff2de9aca5206c4b
f2707ee978e8d6efbe4de0e9b1a93288
11b5f4c84006568d08c6b619f9391e7f
```

- sg_engine_7.5.0.33034_x86-64-small.zip

```
SHA256SUM:
adb01cf6dc9cce09e7a42b6e0e9bfb938a94598c8c13948f4761d79ee48476c0

SHA512SUM:
c18ae996eb1e60e9f3e0310a680475b4
a01a99023d532632c529336ed24ed5c0
a3741af4eb659bf913d9efbdc6e51464
5c3ff122692b174d46952d17afb7fee8
```

- Forcepoint-NGFW-gencloud-7.5.0.33034.ova

```
SHA256SUM:
2fba4d42a40a4c387b166dc9e10f79fbd44384d2ad97ed1efe92d44b3de122bf

SHA512SUM:
f184003c01eabba1762a49c297d95525
8b5c0dd99b644d06a57025b4f6e4aace
72b2feba10459957278423b2e345ee6e
1cd115251d88a54127019eebf1b2f47d
```

- Forcepoint-NGFW-gencloud-7.5.0.33034.qcow2

```
SHA256SUM:
0bcd2445aa63317295b409625ebc04be555a6fa1e4a53ca3a2bf72934e8a96cf

SHA512SUM:
818c8a208908ca11539fa1a1dc6a53b4
3dc613083169d7b23849abe7bd06ef1d
faf4f8245759b3df2153684bc76cbbbe
376c09edf14f4baa4fed51fbcee5497d
```

Compatibility

Security Engine 7.5 is compatible with the following component versions.

- Forcepoint Security Management Center 7.5 or higher
- Dynamic Update 1998 or higher
- Forcepoint VPN Client 6.11.0 or higher for Windows
- Forcepoint VPN Client 2.0.6 or higher for MacOS
- 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 24.04 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*.

IPv6 Support for Modem (LTE/5G) Interfaces

Modem interfaces can now be configured to acquire dynamic IPv6 address.

Multiple LTE/5G APN for Modem interfaces

Added support for configuring multiple LTE/5G Access Point Names (APNs) to enable advanced network connectivity requirements.

Local Web Content Classification for Uncategorized URLs

Added support for real-time methods for local scanning to enable content classification based on the actual web page content when a predefined URL category is not available in the local database. This reduces reliance on cloud queries and minimizes Unknown results. This feature is available in engines with URL Filtering license and 16 GB or more memory. For more details, refer to the *Enable ThreatSeeker* topic in the *Forcepoint Network Security Platform Online Help*.

Quarantine for Malicious Files

Added the ability to quarantine and store malicious files identified by File Filtering policy rules, enabling secure forensic analysis via the Log Server.

Replicate a VPN gateway element from primary engine to secondary engine

Added support to replicate a VPN Gateway from a primary Engine to secondary Engine, enabling shared VPN configuration in policy-based VPN setups. For more details, refer to the *Replicating a VPN Gateway element from the Primary Engine to the Secondary Engine* topic in the *Forcepoint Network Security Platform Online Help*.

Security Engine HA with Policy-Based VPN in Cloud Environments

Enables multiple Engines to share an identical VPN gateway configuration, allowing for seamless failover and load balancing in cloud and disaster recovery environments using the High Availability (HA) script. For more details, refer to the 000012534 Knowledge Base Article.

Traffic Flow Confidentiality

Added support for Precedence Hiding via Differentiated Services Code Point (DSCP) copy restriction and Traffic Flow Confidentiality (TFC) Padding to strengthen data privacy and obfuscate traffic patterns in VPN profiles. For more details, refer to the *Create VPN Profile elements* topic, in the *Forcepoint Network Security Platform Online Help*.

In-band user authentication tracking for HTTP connections

Enables granular user tracking for multi-user hosts and NAT environments by utilizing encrypted HTTP cookies to bind authentication and connection confirmation for specific browser sessions. For more details, refer to the *Browser Session Options* section in the *Define Action options in Access rules* topic, in the *Forcepoint Network Security Platform Online Help*.

Confirm Action in User Response

Added support for a **Confirm** user response action that prompts users before continuing to a target domain and caches their confirmation in an encrypted HTTP cookie to bypass subsequent prompts.

Tagged and Untagged VLANs on the same Physical Interface

Engines now support configuring a native VLAN on physical interfaces, allowing both tagged and untagged traffic to be processed on Layer 3 Physical Interfaces.

Enhancements

This release of the product includes these enhancements.

Enhancements in Security Engine version 7.5.0

Enhancement	Description
DHCPv6 Relay support for client link-layer address option	DHCP relay for IPv6 now adds the client link-layer address option from RFC 6939 by default to relayed DHCPv6 messages.
IKEv2/IPSec Dead Peer Detection (DPD) Enhancement	Added support for configurable DPD Interval (1–28800 seconds) and DPD Timeout (1–300 seconds) values in Gateway Settings to improve IKEv2/IPSec connection monitoring.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 12644.

Security updates

For information about third-party packages and associated vulnerabilities included with the Security Engine in this product release, see Knowledge Base article 12645.

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 7.5 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 7.5 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*.

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 16 June 2026