



Next Generation Firewall

6.9.0

Release Notes

Contents

- [About this release](#) on page 2
- [Lifecycle model](#) on page 2
- [System requirements](#) on page 3
- [Build number and checksums](#) on page 6
- [Compatibility](#) on page 6
- [New features](#) on page 7
- [Enhancements](#) on page 8
- [Resolved and known issues](#) on page 8
- [Installation instructions](#) on page 9
- [Upgrade instructions](#) on page 10
- [Find product documentation](#) on page 10

About this release

This document contains important information about this release of Forcepoint Next Generation Firewall (Forcepoint NGFW). We strongly recommend that you read the entire document.

Lifecycle model

This release of Forcepoint NGFW is a Feature Stream (FS) version.

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

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

For more information about the Forcepoint NGFW lifecycle policy, see <https://support.forcepoint.com/ProductSupportLifeCycle>.

System requirements

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



CAUTION

To protect the privacy of your data, we recommend using dedicated hardware for all NGFW, SMC, and SMC Appliance installations. For cloud-based virtualization platforms, use an instance type that runs on dedicated hardware. For on-premises virtualization platforms, install the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines. For third-party hardware, do not install any other software on the computer where you install the NGFW Engines or SMC components.

Forcepoint NGFW appliances

We strongly recommend using a pre-installed Forcepoint NGFW appliance for Forcepoint NGFW 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 Firewall/VPN, IPS, or Layer 2 Firewall role.

- 50 Series (51 and 51 LTE)
- 100 Series (110 and 115) (*Firewall/VPN role only*)
- 120W
- 320 Series (321 and 325)
- 330 Series (330, 331, and 335)
- 1000 Series (1035 and 1065)
- 1100 Series (1101 and 1105)
- 1402
- 2100 Series (2101 and 2105)
- 3300 Series (3301 and 3305)
- 3400 Series (3401, 3405, and 3410)
- 6205




Note

To use the Forcepoint NGFW Manager, we recommend that you use a Forcepoint NGFW appliance that has at least 4GB of memory.

Basic hardware requirements

You can install Forcepoint NGFW on standard hardware with these basic requirements.

Component	Requirement
CPU	Intel® Pentium D series 2 core or higher
Memory	4 GB RAM
Hard disk	8GB <div>  <div> Note RAID controllers are not supported. </div> </div>
Peripherals	<ul style="list-style-type: none"> ■ DVD drive ■ VGA-compatible display ■ Keyboard
Interfaces	<ul style="list-style-type: none"> ■ One or more network interfaces for the Firewall/VPN role ■ Two or more network interfaces for the IPS in IDS configuration ■ Three or more network interfaces for inline IPS engine or Layer 2 Firewall <p>For information about supported Ethernet interface types and adapters, see Knowledge Base article 9721.</p>

Master NGFW Engine requirements

Master NGFW Engines have specific hardware requirements.

- Each Master NGFW Engine must run on a separate physical device. For more details, see the *Forcepoint Next Generation Firewall Installation Guide*.
- All Virtual NGFW Engines hosted by a Master NGFW Engine or Master NGFW Engine cluster must have the same role and the same Failure Mode (*fail-open* or *fail-close*).
- Master NGFW Engines can allocate VLANs or interfaces to Virtual NGFW Engines. If the Failure Mode of the Virtual IPS engines or Virtual Layer 2 Firewalls is *Normal* (fail-close) and you want to allocate VLANs to several NGFW Engines, you must use the Master NGFW Engine cluster in standby mode.
- Cabling requirements for Master NGFW Engine clusters that host Virtual IPS engines or Layer 2 Firewalls:
 - Failure Mode *Bypass* (fail-open) requires IPS serial cluster cabling.
 - Failure Mode *Normal* (fail-close) requires Layer 2 Firewall cluster cabling.

For more information about cabling, see the *Forcepoint Next Generation Firewall Installation Guide*.

Virtual appliance node requirements

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

Component	Requirement
CPU	Intel® Pentium D series 2 core or higher
Memory	4 GB RAM
Virtual disk space	8 GB
Hypervisor	One of the following: <ul style="list-style-type: none"> ■ VMware ESXi 6.5 or 7.0 ■ KVM with Red Hat Enterprise Linux 7.9 or 8.2 ■ (Firewall/VPN role only) Microsoft Hyper-V on Windows Server 2012 R2 or Windows Server 2016 with an Intel 64-bit processor
Interfaces	<ul style="list-style-type: none"> ■ At least one virtual network interface for the Firewall/VPN role ■ Three virtual network interfaces for IPS or Layer 2 Firewall roles The following network interface card drivers are recommended: <ul style="list-style-type: none"> ■ VMware ESXi platform — <code>vmxnet3</code>. ■ KVM platform — <code>virtio_net</code>.

When Forcepoint NGFW is run as a virtual appliance node in the Firewall/VPN role, 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 Forcepoint NGFW is run as a virtual appliance node in the IPS or Layer 2 Firewall role, clustering is not supported.

Supported cloud environments

You can deploy Forcepoint NGFW in the Amazon Web Services (AWS) and Microsoft Azure cloud environments.

Amazon Web Services

Forcepoint NGFW instances can be launched from AWS using 1-Click Launch, and existing instances can be remotely upgraded to the latest Forcepoint NGFW version.

To see the currently available instance types, search for *Forcepoint NGFW* in the AWS Marketplace.

For more information about deploying in AWS, see the document *How to deploy Next Generation Firewall in the Amazon Web Services cloud* and Knowledge Base article [10156](#).

Microsoft Azure

Forcepoint NGFW instances can be launched from Azure using custom solution templates, and existing instances can be remotely upgraded to the latest Forcepoint NGFW version.

To see the currently available custom solution templates, search for *Forcepoint NGFW* in the Azure Marketplace.

For more information about deploying in Azure, see the document *How to deploy Next Generation Firewall in the Azure cloud* and Knowledge Base article [14485](#).

Build number and checksums

The build number for Forcepoint NGFW 6.9.0 is 25043.

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

- `sg_engine_6.9.0.25043_x86-64-small.iso`

```
SHA1SUM:
11c97cf7a01eb773898574c132c3d737b17ce538

SHA256SUM:
fb0b962523a5884719b79b2414c64434a9f629a1819cda172f6c709c1d9dd23e

SHA512SUM:
e67df16e93c9fd2292406ef7e9815b27
349d7e010f2a5285bc2427c495c12fd8
a8f15b1bb38c48553efb7649dd90ae00
3df841c4ecd588ec6da5afc06bcf66f2
```

- `sg_engine_6.9.0.25043_x86-64-small.zip`

```
SHA1SUM:
dfe2c1a1a4489148f63528d0aa634d86c6b0e107

SHA256SUM:
6e3764fadcd559a1e9a6a12aedc53b72428481ffdf1f04f3e89743808a93952e

SHA512SUM:
3423ef4184df480b2569501935f2cbb6
4231455087ff4dd9267e9275542a6538
918d1afab9c5d7851305941ca6456ad7
1d42b10bb98bf7d3569843d5495b1593
```

Compatibility

Forcepoint NGFW 6.9 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.9 or higher
- Dynamic Update 1298 or higher
- Forcepoint VPN Client for Windows 6.6.0 or higher
- Stonesoft VPN Client for Windows 6.1.0 or higher
- Forcepoint VPN Client for Mac OS X 2.0.0 or higher
- Forcepoint VPN Client for Android 2.0.0 or higher
- Server Pool Monitoring Agent 4.0.0 or higher

- Forcepoint Endpoint Context Agent (ECA) 1.4.0 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 Next Generation Firewall Product Guide*, the *Forcepoint Next Generation Firewall Installation Guide*, and the *Forcepoint NGFW Manager and VPN Broker Product Guide*.

Support for GRE keepalive

The NGFW Engine can now send and reply to keepalive packets in GRE route-based VPN tunnels to check that the GRE tunnel is still functioning. The NGFW Engine sends keepalive packets at the specified interval. If the NGFW Engine does not receive a reply after the specified number of packets, the GRE tunnel is considered to be down.

When you enable GRE keepalive for a tunnel interface on an NGFW Engine, GRE keepalive is used in all GRE route-based VPN tunnels where the tunnel interface is an endpoint.

Log compression for locally managed NGFW Engines

The same log compression options that were previously available in the Management Client are now also available in the Forcepoint NGFW Manager for locally managed NGFW Engines. Log compression prevents excessive log data from being generated and saves resources on the NGFW Engine. When the volume of log entries for antispoofing or discard log events reaches the specified limits, log compression creates a single log entry that contains information about the total number of the generated log entries. After the single log entry is created, logging returns to normal and all generated log entries are logged and shown separately.

Support for IKEv2 Message Fragmentation

Support for IKEv2 Message Fragmentation (RFC 7383) has been added to improve the performance of the Forcepoint VPN Client in networks that do not properly support IP fragmentation. This feature is automatically enabled when the Forcepoint VPN Client connects to NGFW Engine version 6.9 or higher.

Documentation changes

This release of the product includes the following changes to the product documentation:

- The NGFW product documentation is no longer included in the SMC installation files. To find documentation for all Forcepoint products, go to the Forcepoint support website at <https://support.forcepoint.com>.
- The SMC installation files now include automatically generated change log reports for the SMC API in the `api_change_log.zip` file in the `Documentation/SMC_API` folder.
- The title of the *Forcepoint NGFW SMC API Reference Guide* has been changed to *Forcepoint NGFW SMC API User Guide*.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 6.9.0

Enhancement	Description
Configuration of bidirectional forwarding detection using the Management Client	<p>Forcepoint NGFW Engine previously supported the configuration of bidirectional forwarding detection (BFD) using command line tools on the NGFW Engine. You can now configure BFD using the Management Client.</p> <p>When you use the BGP protocol for dynamic routing, you can optionally use BFD to detect neighbor failures. The NGFW Engine sends packets at the specified interval and waits for a reply. If the NGFW Engine does not receive a reply within the specified length of time, the neighbor is considered to have failed.</p>
Enhanced performance probing for Multi-Link VPN tunnels	The internal probing mechanism that monitors the performance of individual Multi-Link VPN tunnels has been enhanced to also work robustly with dynamic VPN endpoints and VPN endpoints that use NAT.
More memory usage details available using SNMP Agents for NGFW Engines	Two new counters for available memory are now reported in Forcepoint NGFW-specific SNMP MIBs. The new OIDs are fwMemBytesAvailable and fwMemBytesSReclaimable. To use the new counters, update the NGFW-specific SNMP MIB for your SNMP tools. For more information, see Knowledge Base article 19210 .
Option to generate one report per sender	When you generate reports, you can now generate one report for each NGFW Engine that is detected as a sender of log data. A new option in the Engine Editor allows you to define the default email addresses to which generated reports are sent when the NGFW Engine is the sender of log data for the report.
Password policy enhancements	The settings for password complexity requirements in the password policy now also apply to SMC administrator accounts that are replicated as local administrator accounts on NGFW Engines, the root account on NGFW Engines, and the Management Server database password.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article [19274](#).

Known limitations

This release of the product includes these known limitations.

Limitation	Description
Inspection in asymmetrically routed networks	In asymmetrically routed networks, using stream-modifying features such as TLS Inspection, URL filtering, and file filtering can make connections stall.

Limitation	Description
Inline Interface disconnect mode	The disconnect mode for Inline Interfaces is supported only on modular appliance models that have full-sized bypass interface modules (not mini modules).

For information about feature-specific limitations, see the *Forcepoint Next Generation Firewall Product Guide*.

Installation instructions

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

For detailed information, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at <https://support.forcepoint.com/Documentation>.



Note

The sgadmin user is reserved for SMC use on Linux, so it must not exist before the SMC is installed for the first time.



Note

If you install the SMC on Windows and Windows Defender is enabled, it might take a long time to activate a dynamic update package. For more information, see Knowledge Base article [14055](#).

Steps

- 1) Install the Management Server, the Log Servers, and optionally the Web Portal Servers.
- 2) Import the licenses for all components.
You can generate licenses at <https://stonesoftlicenses.forcepoint.com>.
- 3) Configure the Firewall, IPS, or Layer 2 Firewall elements in the Management Client from the **Configuration** view.
- 4) To generate initial configurations, right-click each NGFW Engine, then select **Configuration > Save Initial Configuration**.
Make a note of the one-time password.
- 5) Make the initial connection from the NGFW Engines to the Management Server, then enter the one-time password.
- 6) Create and upload a policy on the NGFW Engines in the Management Client.

Upgrade instructions

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



Note

Upgrading to version 6.9 is only supported from version 6.5 or higher. If you have a lower version, first upgrade to version 6.5.



Note

If you use safe search features in NGFW 6.6 or lower, you must refresh the policy on the NGFW Engine cluster after all the members of the cluster have been upgraded to NGFW 6.7 or higher. Otherwise, safe search might not work correctly after the upgrade.

- Forcepoint NGFW version 6.9 requires an updated license. The license upgrade can be requested at <https://stonesoftlicenses.forcepoint.com>. Install the new license using the Management 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 NGFW Engine, use the remote upgrade feature or reboot from the installation DVD and follow the instructions. For detailed instructions, see the *Forcepoint Next Generation Firewall Installation Guide*.

Find product documentation

On the Forcepoint support website, 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 on the Forcepoint support website 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 support website. If you do not yet have credentials, create a customer account. See <https://support.forcepoint.com/CreateAccount>.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint Next Generation Firewall Product Guide*
- Forcepoint Next Generation Firewall 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 Next Generation Firewall Installation Guide*

Other available documents include:

- *Forcepoint Next Generation Firewall Hardware Guide* for your model

- *Forcepoint NGFW Security Management Center Appliance Hardware Guide*
- *Forcepoint Next Generation Firewall Quick Start Guide*
- *Forcepoint NGFW Security Management Center Appliance Quick Start Guide*
- *Forcepoint NGFW SMC API User Guide (Formerly Forcepoint NGFW SMC API Reference Guide)*
- *Forcepoint VPN Client User Guide for Windows or Mac*
- *Forcepoint VPN Client Product Guide*

