



FORCEPOINT

Next Generation Firewall

Release Notes

6.6.3

Revision A

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 issues](#) on page 9
- [Installation instructions](#) on page 10
- [Upgrade instructions](#) on page 11
- [Known issues](#) on page 12
- [Find product documentation](#) on page 12

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*)
- 320 Series (321 and 325)
- 330 Series (330, 331, and 335)
- 1000 Series (1035 and 1065)
- 1100 Series (1101 and 1105)
- 1400 Series (1401 and 1402)
- 2100 Series (2101 and 2105)
- 3200 Series (3202, 3206, and 3207)
- 3300 Series (3301 and 3305)
- 5206
- 6205

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

Component	Requirement
Hard disk	8GB  Note: RAID controllers are not supported.
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

Component	Requirement
Hypervisor	One of the following: <ul style="list-style-type: none"> VMware ESXi 6.5 and 6.7 KVM with Red Hat Enterprise Linux 7.5 and 7.6 Microsoft Hyper-V on Windows Server 2012 or Windows Server 2016 Firewall/VPN role only. An Intel 64-bit processor is required.
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 6.6.3 is 22203.

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

- `sg_engine_6.6.3.22203_x86-64-small.iso`

```
SHA1SUM:
adea5203fe1fe2595bbac3658884efb25bfc46ae

SHA256SUM:
d28daa3edec92507ee14b0dc4bef00da57b700176e0555cc07d893d83c59c269

SHA512SUM:
6317c11cde9c2d97ef30207dbec78e23
2c499e10bca39fa5dbf7d8592827676f
3b76827546995cfbdd9be289fdea67fe
cbf582e53bd0ed101ece0b4cf723c1d4
```

- `sg_engine_6.6.3.22203_x86-64-small.zip`

```
SHA1SUM:
a19608a72fe8295d7aa5852eba64df2c3a77f87a

SHA256SUM:
20e00e8bc94d977e1ac3c5505946be0210fbd935274a614533dae4cb41b2a392

SHA512SUM:
4c9a927b9a29313697c566fa85fcfe5f
5fbb816a4219e892306ba9f8a2e58f33
32ae019c5494d5c8428297e83d57abc8
422b9af57b8e78f3579eddc4c4478af7
```

Compatibility

Forcepoint NGFW 6.6 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.6 or higher
- Dynamic Update 1145 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) 1.1.0 or higher
- Forcepoint User ID Service 1.1.0 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* and the *Forcepoint Next Generation Firewall Installation Guide*.

Dynamic link selection for SD-WAN

The VPN links that are used for Multi-Link traffic from applications and protocols, and traffic associated with QoS classes are now automatically selected based on quality metrics defined for the network applications, protocols, and QoS classes. You can now also specify how different types of ISP connections are used for specific types of traffic. For each type of ISP connection, you can specify that:

- The ISP connection is used for the specified type of traffic unless an ISP connection with significantly higher quality is available.
- The ISP connection is used for the specified type of traffic only if the quality of the other ISP connections is too low or the other ISP connections are not available.
- The ISP connection must not be used for the specified type of traffic.

Storage and browsing of log data locally on NGFW Engines

You can now save copies of the most recent log entries locally on the NGFW Engine. Alert entries are also saved locally on the NGFW Engine. You can browse the saved log and alert entries on the command line of the NGFW Engine even if the log and alert entries have already been sent to the Log Server. The length of time for which the log and alert entries are stored depends on the size of the NGFW Engine's disk and the volume of log data. You can also set limits for how long log entries are stored, and how much disk space can be used for storage.

LLDP support

NGFW Engines can now use the Link Layer Discovery Protocol (LLDP) to send information, such as information about interfaces and MAC addresses on the NGFW Engine, to directly connected devices on the network. The NGFW Engines can also receive information that other devices on the network send. In the Management Client, you can now monitor information that the NGFW Engine has received about devices in directly connected networks.


Support for LTE modems on NGFW Engines in the Firewall/VPN role

You can now use LTE modems for mobile broadband connections on 4G networks with NGFW Engines in the Firewall/VPN role. Support for LTE modems is only available on specific purpose-built NGFW appliance models (NGFW 50 Series).

Enhancements


This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 6.6.0

Enhancement	Description
Easier forwarding to a proxy	You can now configure forwarding traffic to a proxy or host directly in the Access rules rather than in the NAT rules.
Shared interfaces on Master NGFW Engines	<p>Layer 3 physical interfaces on Master NGFW Engines in the Firewall/VPN role can now be shared interfaces.</p> <ul style="list-style-type: none"> You can now connect Virtual Firewalls to the same network without dedicating one physical interface or VLAN for each Virtual Firewall. The Virtual Firewalls can now communicate with each other without an external switch or router. Link aggregation is supported on Virtual Firewalls.
IPv6 support for user authentication	User authentication now supports IPv6 addresses. Communication between NGFW Engines and authentication servers now also supports IPv6 addresses.
Server Pool enhancements	<p>The following enhancements have been made for the Server Pool feature:</p> <ul style="list-style-type: none"> You can now use Server Pool elements in NAT rules to apply both source and destination NAT for Server Pool load balancing. The Server Pool feature now supports IPv6.
New URLs for dynamic updates and engine upgrades	<p>To improve the performance of automatic dynamic updates and engine upgrades, the following new URLs are available in SMC 6.5.0 and higher:</p> <ul style="list-style-type: none"> https://autoupdate.ngfw.forcepoint.com/dynup.rss https://autoupdate.ngfw.forcepoint.com/ngfw.rss <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note: The SMC automatically starts using the new URLs when you upgrade to SMC 6.5.0 or higher and activate the dynamic update package that includes the new URLs.</p> </div> <p>The new URLs use a content distribution network (CDN) to allow the SMC to download dynamic update packages and engine upgrade files from the geographically closest server. The legacy https://update-pool.stonesoft.com/index.rss URL remains available for backward compatibility and as a backup for the new URLs.</p>
Configurable update services for dynamic updates and engine upgrades	<p>New Update Service elements define sets of URLs for automatic dynamic updates and engine upgrades. In SMC 6.5.0 and higher, the SMC automatically uses Update Service elements that include both the new URLs and the legacy URL. No action is needed to start using the Update Service elements that include the new URLs.</p> <p>Starting from SMC 6.5.2, you can optionally change which Update Service element is used for automatic dynamic updates and engine upgrades. For more information, see Knowledge Base article 16589.</p>

Enhancement	Description
Application routing improvements	Application routing is now more flexible and can process network applications where the server sends data first.
IPsec VPN performance improvements	IPsec VPN performance has improved significantly. For example, when the AES-GCM-256 encryption method is used, the maximum throughput has increased by up to 300%.

Enhancements in Forcepoint NGFW version 6.6.1

Enhancement	Description
Forward Error Correction (FEC) mode for Multi-Link VPNs	<p>When packet loss is detected on a NetLink in a Multi-Link VPN, FEC duplicates packets on that link to ensure that there is no packet loss. FEC is applied to traffic according to the QoS Class of the traffic.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Note: Excessive packet duplication can saturate the link capacity. Make sure to apply FEC only to traffic that requires it.</p> </div>
New syntax for CN field in certificate requests for browser-based user authentication	It is now possible to use a specific syntax for the CN field in a certificate request (CSR) for browser-based user authentication so that the Subject Alternative Name (SAN) fields can already be defined when the NGFW Engine generates the certificate request for browser-based user authentication. For more information, see Knowledge Base article 17375 .

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in a previous release, see the Release Notes for the specific release.

Description	Role	Issue number
In environments with many VPNs that use certificate-based authentication, there might be messages about missing certificates during policy installation and the VPNs might not be functional, even if the certificates are available.	FW	NGFW-16595
When many Sidewinder Proxies are configured, policy installation might take too long and traffic that is processed through the proxies might stop.	FW	NGFW-19012
WebSocket Server Stream situations are not correctly identified in traffic.	FW, IPS, L2FW	NGFW-19443
When traffic is matched against a Network Application and Zones are in use, outgoing connections might match against the wrong Access rule if the Zone changes due to destination NAT being applied.	FW	NGFW-19860
When an NGFW Engine cluster starts using a new certificate for certificate-based authentication in a VPN, the certificate might not work on all nodes of the cluster.	FW	NGFW-19932
An NGFW Engine installed on a C5 instance in Amazon Web Services (AWS) might restart.	FW	NGFW-20029

Description	Role	Issue number
In the action options of an Access rule, the value for the Enforce TCP MSS option is not taken into account if application routing is in use.	FW	NGFW-20039
After you activate a new dynamic update, policy installation requires more memory than normal to handle new fingerprint DFAs. The memory allocation for the inspection process might fail, causing the inspection process to restart during the policy installation. The NGFW Engine might also restart.	FW, IPS, L2FW	NGFW-20230
Valid SSH connections might incorrectly match the SSH_Violation situation when application logging is enabled for the traffic.	FW, IPS, L2FW	NGFW-20250
The inspection process might restart.	FW, IPS, L2FW	NGFW-20440
In an environment with Master NGFW Engines and Virtual NGFW Engines, SSL VPN tunnels work only on one Virtual NGFW Engine.	FW	NGFW-20602
In an NGFW Engine cluster, full state synchronization messages might be sent as burst traffic, causing the recipient to be unable to handle all the packets. You might see the FW_Synchronization-State-Sync-Failed-To-Receive Situation in log entries.	FW, IPS, L2FW	NGFW-20635
In Multi-Link VPNs, when an endpoint that has a dynamic IP address uses an IP address as the Phase-1 identity, connections might not be transferred to the VPN link when another VPN link is not available.	FW	NGFW-20860
In SMC 6.6.2 or higher, traffic might match the wrong rule if the policy includes an Access rule in which the action options are set to forward traffic.	FW	NGFW-20968
In rare cases when you use file filtering, TLS inspection, or URL categorization, the NGFW Engine might keep connections open in the TCP Close Wait state indefinitely. As a result, the NGFW Engine might run out of memory.	FW, IPS, L2FW	NGFW-21013
When an NGFW Engine has more than 64 VLANs configured and you add or delete a VLAN, the change is not applied even though policy installation succeeds. Changes to the VLAN configuration are applied only when you restart the NGFW Engine.	FW, IPS, L2FW	NGFW-21868

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 6.6 is only supported from version 6.3 or higher. If you have a lower version, first upgrade to version 6.3.



Note: Starting from Forcepoint NGFW version 6.4, the McAfee Advanced Threat Defense feature is no longer supported. We recommend that you use Forcepoint Advanced Malware Detection instead.

- Forcepoint NGFW version 6.6 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*.
- If you have customized the `sshd_config` file in the `/data/config/ssh` directory, you might need to manually update the configuration file after upgrading the NGFW Engine to Forcepoint NGFW version 6.6. See Knowledge Base article [10461](#).

Known issues

For a list of known issues in this product release, see Knowledge Base article [16954](#).

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.
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*.

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, Knowledge Base articles, downloads, cases, and contact information.

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 Reference Guide*

- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*

