



# Next Generation Firewall

6.7.3

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 7
- [Resolved issues](#) on page 8
- [Installation instructions](#) on page 10
- [Upgrade instructions](#) on page 11
- [Known issues](#) on page 11
- [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)
- 3207
- 3300 Series (3301 and 3305)
- 3400 Series ( 3401, 3405, and 3410)
- 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  <b>Note</b> RAID controllers are not supported.
Peripherals	<ul style="list-style-type: none"> <li>■ DVD drive</li> <li>■ VGA-compatible display</li> <li>■ Keyboard</li> </ul>
Interfaces	<ul style="list-style-type: none"> <li>■ One or more network interfaces for the Firewall/VPN role</li> <li>■ Two or more network interfaces for the IPS in IDS configuration</li> <li>■ Three or more network interfaces for inline IPS engine or Layer 2 Firewall</li> </ul> For information about supported Ethernet interface types and adapters, see Knowledge Base article <a href="#">9721</a> .

## 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"> <li>■ VMware ESXi 6.5 or 6.7</li> <li>■ KVM with Red Hat Enterprise Linux 7.7 or 8.0</li> <li>■ (Firewall/VPN role only) Microsoft Hyper-V on Windows Server 2012 or Windows Server 2016 with an Intel 64-bit processor</li> </ul>
Interfaces	<ul style="list-style-type: none"> <li>■ At least one virtual network interface for the Firewall/VPN role</li> <li>■ Three virtual network interfaces for IPS or Layer 2 Firewall roles</li> </ul> The following network interface card drivers are recommended: <ul style="list-style-type: none"> <li>■ VMware ESXi platform — <code>vmxnet3</code>.</li> <li>■ KVM platform — <code>virtio_net</code>.</li> </ul>

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 6.7.3 is 23154.

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

- `sg_engine_6.7.3.23154_x86-64-small.iso`

```
SHA1SUM:
afa7a69873e484215c77df86a50c2f1181cd181c

SHA256SUM:
e3da7f8bb7db639286a80770e0c97eec23cf1fcccb0fda3074ff160d4da400ed

SHA512SUM:
009df10fc3f2fe114a01882d175470d4
9cf3f123645a2abbb24f54865d8ff6ba
bbe3c64b83f79ebaf82cd038bd837ea4
61e25157ad81fbfd9b77307fa2aeb017
```

- `sg_engine_6.7.3.23154_x86-64-small.zip`

```
SHA1SUM:
1493215103f6f024094be0afef966c90bd161372

SHA256SUM:
62c5d0e4974af999d9701336ad6ecdf4c071930d3d7d784b808d8dd0b9b423e8

SHA512SUM:
00cc772745d2b5bf77e8bccbe96fbc33
b0cfa0d0295740bdb4dbe52fd857cb12
86d887a288aeb4fcf12488c5422880f
aaf5419921fb8f0fc488aa89c9dca887
```

## Compatibility

Forcepoint NGFW 6.7 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.7 or higher
- Dynamic Update 1196 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*.

## VPN Broker

The VPN Broker is a new component of Forcepoint NGFW. As part of an SD-WAN solution, the VPN Broker creates highly-scalable, full-mesh VPN environments without the need for complex dynamic routing configurations. VPN tunnels are automatically created between NGFW Engines when they communicate with each other, and automatically removed when they are no longer needed.

You can configure the VPN Broker in the NGFW Manager on a dedicated Forcepoint NGFW appliance. You can configure the VPN Broker as a single VPN Broker or as part of a high availability VPN Broker configuration.

For more information about the VPN Broker, see the *Forcepoint NGFW Manager and VPN Broker Product Guide*.

## On-premises DLP integration

You can now integrate ICAP servers with Forcepoint NGFW to provide DLP scanning in the File Filtering Policy for outbound file transfers.

There are some limitations when you use ICAP servers with Forcepoint NGFW for DLP scanning. For more information, see Knowledge Base article [17727](#).

# Enhancements

This release of the product includes these enhancements.

## Enhancements in Forcepoint NGFW version 6.7.0

Enhancement	Description
Improved inspection of HTTP/2 traffic	The inspection of HTTP/2 traffic has been improved. HTTP/2 is no longer downgraded to HTTP for inspection.
Improvements to rule validity time configuration	<p>New options for defining rule validity time allow you to define rule validity time more precisely. It is now also possible to define when individual rules start being enforced, and when the rules automatically expire.</p> <p>When you upgrade to version 6.7, existing rule validity times are automatically converted to use the new rule validity time options. However, some previous rule validity time options are no longer supported in version 6.7 and higher. If you used rule validity times in a previous version, check your policies to make sure that the rule validity time options match as intended.</p>

Enhancement	Description
Optimization of URL categories	<p>When you upgrade to SMC 6.7 or higher, URL categories are optimized and reorganized into five top-level URL Category Groups:</p> <ul style="list-style-type: none"> <li>■ <b>Security</b> — Group of categories known to pose a security threat</li> <li>■ <b>Reputation</b> — Group of categories that might have security implications</li> <li>■ <b>Legal Liability</b> — Group of categories that contain content related to a potential age restriction or legal infringement</li> <li>■ <b>Bandwidth</b> — Group of categories known to consume bandwidth resources</li> <li>■ <b>Baseline</b> — Group of categories related to general web access traffic</li> </ul> <p>Action might be needed if you have enabled ThreatSeeker for URL categorization for an NGFW Engine in the Engine Editor and you use ThreatSeeker categories for URL filtering in Access rules. For more information, see Knowledge Base article <a href="#">17133</a>.</p>
QinQ inspection support	Deep inspection now supports inspection of double-tagged VLAN (QinQ) traffic with layer 2 interfaces in inline or capture mode.

## Enhancements in Forcepoint NGFW version 6.7.3

Enhancement	Description
Improved VPN performance	VPN performance has been improved in environments where there is a high rate of new VPN connections.
Support for ACPI shutdown	Support for advanced configuration and power interface (ACPI) shutdown has been implemented. This feature allows graceful shutdown when terminating virtual instances in the Microsoft Azure and Amazon Web Services platforms.

## 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 NGFW Engine clusters, when an interface that has DHCP relay enabled is also selected as the Default IP Address for Outgoing Traffic, DHCP requests might go out through the incorrect interface if there are interfaces without NDI addresses.	FW	NGFW-2657
In an SD-WAN environment where QoS is used for dynamic link selection, memory usage becomes excessive over time.	FW	NGFW-23593
In rare cases, the VPN process might restart.	FW	NGFW-25714
Power supply monitoring for NGFW appliances might trigger an alert even though the status of the power supply is OK.	FW, IPS, L2FW	NGFW-25942
When policy installation has previously failed, the inspection process might restart during a later policy installation.	FW, IPS, L2FW	NGFW-26042



Description	Role	Issue number
The counters for natted traffic and dropped traffic might provide incorrect data in overviews.	FW	NGFW-26142
When you use URL categorization, the inspection process might restart when the NGFW Engine processes malformed HTTP/2 traffic.	FW, IPS, L2FW	NGFW-26200
When you use DLP integration, the ICAP X-Authenticated-User header does not include users in the format WinNT://<domain>/<user>.	FW, IPS, L2FW	NGFW-26280
When an NGFW Engine cluster uses load-balanced clustering and traffic that is encrypted in a GRE tunnel is terminated at the NGFW Engine, the traffic might be rejected. For example, BGP connections might be affected.	FW	NGFW-26385
Mobile VPN sessions with a large number of authentication groups for a user might cause the state synchronization process to restart.	FW	NGFW-26472
When Global Threat Intelligence is enabled but the NGFW Engine has been without DNS access for an extended time, the NGFW Engine might restart after policy installation.	FW, IPS, L2FW	NGFW-26558
Compressed logs with the Log_Compress-SIDs situation do not include rule tags.	FW, IPS, L2FW	NGFW-26597
When you use the Integrated User ID Service, the NGFW Engine might stop processing traffic.	FW, IPS, L2FW	NGFW-26598
In route-based VPN tunnels between NGFW Engines in the Firewall/VPN role, if one endpoint has a FQDN as the contact address and NAT is applied to the private IP address of the endpoint, VPN monitoring probes are sent to the wrong IP address on the endpoint that has an FQDN contact address.	FW	NGFW-26601
Deleted link-local IPv6 addresses remain on the interface.	FW	NGFW-26672
Certificate CRL verification might stop working.	FW, IPS, L2FW	NGFW-26875
When an NGFW Engine cluster uses load-balanced clustering, connections from VPN Clients might not be correctly forwarded to other VPN tunnels.	FW	NGFW-27271
The results of DLP scans using ICAP for file filtering are cached. If one user was recently allowed to access content, a new DLP scan request might not be sent when another user tries to access the same content. As a result, users who were not intended to be allowed to access to the content might be allowed to access it.	FW, IPS, L2FW	NGFW-27372
BGP routes are deleted when an update message that includes same address prefix in the withdrawn routes and Network Layer Reachability Information fields is received.	FW	NGFW-27418
When you use Virtual NGFW Engines on NGFW Appliances with limited RAM, policy installation might fail if policies that include different dynamic update packages are installed on different Virtual NGFW Engines.	FW, IPS, L2FW	NGFW-27435
When the NGFW Engine is inspecting a TCP connection that has inconsistent sequence numbers, the inspection process might restart. Capture interfaces are most likely to receive packets that have inconsistent sequence numbers.	FW, IPS, L2FW	NGFW-27633
When there are large bursts of user group membership updates in ECA, ECA state sync might log the following error: "Resource temporarily unavailable State sync internal communication error".	FW, IPS, L2FW	NGFW-27679
When the NGFW Engine is handling SIP UDP traffic, the inspection process might restart.	FW, IPS, L2FW	NGFW-27725

Description	Role	Issue number
When you use the multicast MAC clustering mode, nodes incorrectly reply to ARP requests about CVI addresses.	FW	NGFW-28019
In rare cases, the NGFW Engine might restart.	FW, IPS, L2FW	NGFW-28252
The "Any Network" element and overlapping networks on VPN Broker Members might not be handled correctly.	FW	NGFW-28381
SNMP monitoring for VPN SAs always returns 0 as the value.	FW	NGFW-28392

## 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 6.7 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.



## Note

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

- Forcepoint NGFW version 6.7 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 6.7. See Knowledge Base article [10461](#).

## Known issues

For a list of known issues in this product release, see Knowledge Base article [17719](#).

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

