



FORCEPOINT

Next Generation Firewall

Release Notes

6.7.1

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 7
- [Resolved issues](#) on page 8
- [Installation instructions](#) on page 11
- [Upgrade instructions](#) on page 12
- [Known issues](#) on page 12
- [Find product documentation](#) on page 13

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)
- 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 For information about supported Ethernet interface types and adapters, see Knowledge Base article 9721 .

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 or 6.7 KVM with Red Hat Enterprise Linux 7.7 or 8.0 (Firewall/VPN role only) Microsoft Hyper-V on Windows Server 2012 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 6.7.1 is 23055.

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

- `sg_engine_6.7.1.23055_x86-64-small.iso`

```
SHA1SUM:
c0a45b5db2ddc91dd7887f0f57f47fafe6fbe59f

SHA256SUM:
4bfe7025158ab9a0f955e0af45b1926ac3a810da66d12abe2f977e7d880888ed

SHA512SUM:
2e8e228cf4fbc44880173b32ce2e1b89
70c7f055b6586de6df03eb1bed4b68a4
e56935750f86ac9a1b854a5061a19e0b
af48ca176f232322ca133c2d21fba73c
```

- `sg_engine_6.7.1.23055_x86-64-small.zip`

```
SHA1SUM:
e289e1ffce5dc4d5fff184063e48b3148a65bd28

SHA256SUM:
862b524a5387a9115c8eae86dfe37dd2401590b53cd92b5585200e246e2a6229

SHA512SUM:
6ffcae5a150b563693c9fc60ee04c06e
20d7abfb3b8d19f6ecf3b4b39db7febc
218534ef3a90fd3381fbefb2dc62015a
03b655956421ff60a2829d76d89d7c59
```

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"> • Security — Group of categories known to pose a security threat • Reputation — Group of categories that might have security implications • Legal Liability — Group of categories that contain content related to a potential age restriction or legal infringement • Bandwidth — Group of categories known to consume bandwidth resources • Baseline — Group of categories related to general web access traffic <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 17133.</p>
QinQ inspection support	Deep inspection now supports inspection of double-tagged VLAN (QinQ) traffic with layer 2 interfaces in inline or capture mode.

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
If the Multiple Virtual Resources option is enabled on an interface for a Master NGFW Engine, and you add additional Virtual Resources to a VLAN interface that already has a Virtual Resource configured, then add IP addresses for the Virtual NGFW Engines, when you install the policy, the new IP addresses are not included in the configuration.	FW, IPS, L2FW	NGFW-17697
When you add an aggregated interface to a Master NGFW Engine, the link status might show that the link is down.	FW, IPS, L2FW	NGFW-17699
The SD-WAN dashboard might show an incorrect value for packet loss rate for a VPN tunnel.	FW	NGFW-18962
File filtering might not block a file reliably based on MD5SUM or SHA1SUM checksums if the client requests a file in several parts and the delay between downloading the parts is too long.	FW, IPS, L2FW	NGFW-19194
When a rule that has rule validity specified allows a connection, the connection is discarded when the rule is no longer valid. The connection is not matched against other rules in the policy that might otherwise allow the connection.	FW, IPS, L2FW	NGFW-19907
When using Global Threat Intelligence (GTI), you might frequently see the information message "GTI not available" in log entries.	FW, IPS, L2FW	NGFW-20155
In a Session Initiation Protocol (SIP) control connection, the NGFW Engine does not translate the address and port information in the Via header when NAT is applied to the connection.	FW	NGFW-20346

Description	Role	Issue number
When you first install a policy on the N51L appliance model with LTE configured, the installation might fail. The following message is shown: syntax error in network configuration: DHCP parameter lookup failure.	FW	NGFW-21460
Deep inspection of IPv6 traffic may generate IPv6 flow labels incorrectly.	FW, IPS, L2FW	NGFW-21554
When there is heavy VPN traffic load, policy installation on the NGFW Engine might become unresponsive. When the VPN process is delayed to apply the new policy, there can be an impact on traffic.	FW	NGFW-22111
Inspection rules might incorrectly block valid HTTP/2 traffic.	FW, IPS, L2FW	NGFW-22345
In an environment with Multi-Link VPN tunnels that use an FQDN that resolves to both an IPv4 and IPv6 address, when you view the status of VPN tunnels in the SD-WAN dashboard, the health value for a VPN tunnel might be low and shown as red.	FW	NGFW-22504
If a Master NGFW Engine has a shared interface, traffic between the Virtual NGFW Engines does not work if the Virtual NGFW Engines are active on different cluster nodes, and the physical interface uses the i40e driver.	FW, IPS, L2FW	NGFW-22549
International characters in the Display Name field of a SIP message can cause SIP calls to not work.	FW, IPS, L2FW	NGFW-22677
If load-balancing is used on a clustered NGFW Engine, some connections might fail if destination NAT is applied to the connections and the translated IP addresses are also used for dynamic NAT.	FW	NGFW-22697
When the NGFW Engine processes HTTP/2 traffic, the inspection process might restart or the processing of the connection might stop.	FW, IPS, L2FW	NGFW-22724
Connections that match a rule that uses a Service for a Sidewinder Proxy might fail if the connection is allowed by a Destination Zone match.	FW	NGFW-22762
If a monitoring probe has been configured for a route from a tunnel interface, but the tunnel interface is not included in any route-based VPN tunnel, all monitoring probes fail.	FW	NGFW-22874
No warning about BGP misconfiguration is shown if both a prefix and a distribution list have been configured for BGP peers.	FW	NGFW-22956
In a Multi-Link VPN setup, traffic that has failed over to a standby NetLink might not be transferred back to the active NetLink as expected when the active NetLink becomes usable again.	FW	NGFW-23050
When you use load balancing clustering, the BGP routing protocol does not work reliably with tunnel interfaces for route-based VPNs.	FW	NGFW-23055
On the N51L appliance model, the LTE interface does not handle incoming IPv6 traffic correctly. The traffic is dropped by antispoofing.	FW	NGFW-23242
If packets in a VPN tunnel are fragmented, the reassembling of the arriving fragments might fail.	FW	NGFW-23333
The option Always Keep Tunnels Established might not work as expected when the NGFW Engine is the Phase-2 responder in a VPN negotiation.	FW	NGFW-23349

Description	Role	Issue number
In an environment where the total number of Management Servers, Management Server contact addresses, and NGFW Engine control interfaces is high, but not all the Management Server contact addresses are reachable, it might take a long time before NGFW Engines with dynamic IP addresses are reachable after management connection has been lost.	FW, IPS, L2FW	NGFW-23471
The SNMP monitoring process might restart if a large number of interfaces is queried.	FW, IPS, L2FW	NGFW-23735
Repeated SIP invite requests in a SIP connection might prevent NAT for related connections.	FW	NGFW-23756
When application routing and outbound balancing of traffic is in use, the inspection process or the NGFW Engine might restart.	FW	NGFW-23886
During the inspection of HTTPS traffic, the TLS session cache can increase in size over time. When the TLS session cache tries to reduce memory usage, it might fail and cause the inspection process to restart.	FW, IPS, L2FW	NGFW-23906
The Blacklist Monitoring view might show blacklist entries that no longer exist if log data has been temporarily spooled on the NGFW Engine.	FW, IPS, L2FW	NGFW-24014
Apple devices expect TLS certificates to have the Enhanced Key Usage extension. When TLS decryption is used, the NGFW Engine does not include this extension in the certificate that is provided to the client.	FW, IPS, L2FW	NGFW-24030
When the external authentication servers for browser-based user authentication are not responding or respond very slowly and many listening interfaces are configured on the NGFW Engine, the logon page for browser-based user authentication might load slowly or not at all.	FW	NGFW-24111
In an NGFW Engine cluster, a state synchronization packet might become fragmented in a way where the last packet is very small and arrives at the other node first. The NGFW Engine shows an excessive number of log entries that have the message "Failed to receive sync message error".	FW, IPS, L2FW	NGFW-24152
A Virtual NGFW Engine might use an incorrect MAC address on an IPv4 proxy ARP when an interface on the Master NGFW Engine is assigned to a Virtual Resource and VLAN creation is allowed.	FW	NGFW-24175
When the NGFW Engine uses file filtering, it might send packets that are larger than the maximum segment size (MSS) on both sides.	FW	NGFW-24224
With a large VPN configuration, the VPN process might stop responding during the policy installation, causing the NGFW Engine to restart.	FW	NGFW-24239
User Responses do not work with HTTP/2 TLS traffic.	FW, IPS, L2FW	NGFW-24242
If you have configured BGP routing for an NGFW Engine cluster, policy installation might fail.	FW	NGFW-24288
Upgrading the NGFW Engine remotely immediately after making initial contact might fail. The upgrade is successful if you restart the NGFW Engine after making initial contact.	FW, IPS, L2FW	NGFW-24323
In rare cases, blacklisting might not work correctly on Virtual NGFW Engines.	FW, IPS, L2FW	NGFW-24327
There are several issues related to the VPN Broker.	FW	NGFW-24337

Description	Role	Issue number
A configuration where the primary and backup heartbeat interfaces have different MTU values is allowed by the NGFW Engine. If the primary heartbeat interface has a larger MTU value, when the connection fails over to the backup heartbeat interface, one of the nodes might go offline, and the message "failed to sync cluster state with it" is shown.	FW, IPS, L2FW	NGFW-24367
SSL VPN tunnel connections might be discarded when a policy is installed.	FW	NGFW-24447

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, 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*

