FORCEPOINT

Next Generation Firewall

Release Notes

6.7.2

Revision B

Contents

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 **Note:** RAID controllers are not supported.
Peripherals	• DVD drive • VGA-compatible display • Keyboard
Interfaces	• 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: • 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	• 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: • VMware ESXi platform — `vmxnet3`. • KVM platform — `virtio_net`.

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 6.7.2 is 23105.

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

- sg_engine_6.7.2.23105_x86-64-small.iso

```
SHA1SUM:
2ef5e047087b3c79dc5de4aeb5850e2cf1d46782

SHA256SUM:
6fff402ebd23b09630014e10b9a43992aa3cac30c4ac3d258d71c4e8b69eb3d7

SHA512SUM:
ad18daaabbbfb9e2becbef6ddbe3ba04
4c74fce8f38379d5c1b0ceaacd81077c
6c18fc8aa4a20e61c187ef77b3c1e97a
27499f2cc1316db398396d678e80c393
```

- sg_engine_6.7.2.23105_x86-64-small.zip

```
SHA1SUM:
f6d771a014f92577507f20059c0da0b22ed65de1

SHA256SUM:
548e40c998cea11aae1a341175f977057ccf91f6925836e6ec846f6d97cae7c1

SHA512SUM:
e0191481fe89366d5ac3fcf4afb1030c
7635804eba2eb40244762067a734f8d2
789484bffdc3ed4a1b3f183f0e0a45fc
76e2d1f4e48943c6e3fa4f5f5f4e4313
```

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	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. 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.

Enhancement	Description
Optimization of URL categories	When you upgrade to SMC 6.7 or higher, URL categories are optimized and reorganized into five top-level URL Category Groups: • **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 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.
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
To address https://support.microsoft.com/en-us/help/4049215/extensions-and-virtual-machine-agent-minimum-version-support, waagent is updated to version 2.2.45.	FW, IPS, L2FW	NGFW-17710
In large VPN configurations, the NGFW Engine node might become unresponsive or restart when you install a policy that includes changes to the VPN configuration.	FW	NGFW-18644
Incoming traffic to a shared interface on a Master NGFW Engine might cause the Master NGFW Engine to restart.	FW, IPS, L2FW	NGFW-23399
When there are a large number of new VPN connections, processing the connections might slow down.	FW	NGFW-23932
When thousands of VPN tunnels are configured, new VPN connections are matched inefficiently to VPN tunnels.	FW	NGFW-24064
If there is a large number of DHCP relay interfaces, some of the DHCP relay interfaces might not work correctly.	FW	NGFW-24107
When you change the netmask of an interface that has a default route configured, the default route is removed from the routing table.	FW	NGFW-24134
When inspection is enabled for TLS connections, TLS 1.3 connections might fail. The TLS_Unrecoverable-Error situation might appear in log entries.	FW, IPS, L2FW	NGFW-24144
The Tunnels pane in the SD-WAN dashboard might show incorrect values.	FW	NGFW-24469
When you add more than one network that is configured on the same interface, only one of the networks is included in the OSPF configuration.	FW	NGFW-24597

Description	Role	Issue number
VPN Broker members do not always send endpoint information to the VPN Broker gateway. There are also other minor issues related to the VPN Broker.	FW	NGFW-24827
In rare cases, the VPN process might cause the NGFW Engine node to restart.	FW	NGFW-24974
A user response is not always shown when TLS connections are blocked.	FW, IPS, L2FW	NGFW-25112
In large VPN configurations, the NGFW Engine node might go offline, or its operation might slow down. The following message is shown in the dmesg output "NGFW: memory allocation of X bytes failed".	FW	NGFW-25125
Using a user response to redirect HTTP/2 traffic to the logon page for browser-based user authentication does not work correctly.	FW	NGFW-25199
When an NGFW Engine has hundreds of interfaces configured, the NGFW Engine might restart.	FW, IPS, L2FW	NGFW-25218
When a rule is configured to only log that termination of matching traffic could have occurred, receiving file ranges out of order might cause the inspection process to restart.	FW, IPS, L2FW	NGFW-25238
Protocol identification might cause some connections to be buffered unnecessarily, resulting in low throughput for the connections.	FW, IPS, L2FW	NGFW-25718
When you use application routing, the inspection process might restart if the route changes during connection closing.	FW, IPS, L2FW	NGFW-25852
When there is fragmented traffic, the NGFW Engine might restart when you install a policy that includes changes to the interface configuration.	FW, IPS, L2FW	NGFW-25900
When VLANs that host multiple Virtual NGFW Engines are configured on a Master NGFW Engine interface that has an i40e driver, communication between Virtual NGFW Engines might fail if the Virtual NGFW Engines are active on different Master NGFW Engine nodes.	FW	NGFW-25965

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.

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*

Published 27 April 2020