Next Generation Firewall

Release Notes

6.6.6

Revision A

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)
- 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	• 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 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	- 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 6.6.6 is 22352.

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

- sg_engine_6.6.6.22352_x86-64-small.iso

  ```
  SHA1SUM:
  303ab52e9fbb7706ba2cc4f07904e87a3614f7e7

  SHA256SUM:
  b50a37cfc9e0ad8e70b595f4d92a07603e927b823f02e14be132abf20b4502fc

  SHA512SUM:
  d7787747d08eaa2bd66b9c44782abb11
  cad9625d92018ec93f8c969cc16d550c
  76adbf5ff7f897c9fbda442789458457
  f78f45f3b1938364b3fe46f581b482b5
  ```

- sg_engine_6.6.6.22352_x86-64-small.zip

  ```
  SHA1SUM:
  a0b3af480330f2e5dafb605ae36f3858ff3ba739

  SHA256SUM:
  8a88997b344ccdde93e9032369fc679f0d87482b04e9d7b4403cee9fea25a91e

  SHA512SUM:
  0b0ec3b89fd6343cecaef9d1166b270a
  e1230c35a3104668159c1b700ddfe1d3
  db339e44588796222521218f135d3075
  03810d199622e6463d7bba8bf2380908
  ```

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	Layer 3 physical interfaces on Master NGFW Engines in the Firewall/VPN role can now be shared interfaces. • 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	The following enhancements have been made for the Server Pool feature: • 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	To improve the performance of automatic dynamic updates and engine upgrades, the following new URLs are available in SMC 6.5.0 and higher: • https://autoupdate.ngfw.forcepoint.com/dynup.rss • https://autoupdate.ngfw.forcepoint.com/ngfw.rss **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. 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.
Configurable update services for dynamic updates and engine upgrades	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. 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.

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	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. **Note:** Excessive packet duplication can saturate the link capacity. Make sure to apply FEC only to traffic that requires it.
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.

Enhancements in Forcepoint NGFW version 6.6.4

Enhancement	Description
Support for YouTube in DNS-based SafeSearch	DNS-based SafeSearch has been extended to support YouTube.

Enhancements in Forcepoint NGFW version 6.6.6

Enhancement	Description
ACPI shutdown support	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
The IPsec VPN facility logs user names in the format user@domain instead of using the separate User and User Domain log fields.	FW	NGFW-17317
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 an SD-WAN environment where QoS is used for dynamic link selection, memory usage becomes excessive over time.	FW	NGFW-23593
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
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
The Tunnels pane in the SD-WAN dashboard might show incorrect values.	FW	NGFW-24469
The URL category might not always be included in the user response when a URL is not allowed for HTTPS traffic.	FW, IPS, L2FW	NGFW-24703
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
In rare cases, the VPN process might restart.	FW	NGFW-25714
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
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
If the VPN configuration includes a large number of endpoints with dynamic IP addresses, new policy installation for the VPN process might be slow. As a result, a node in the cluster might go offline.	FW	NGFW-26403

Description	Role	Issue number
Mobile VPN sessions with a large number of authentication groups for a user might cause the state synchronization process to restart.	FW	NGFW-26472
In an environment with a large number of dynamic routes, synchronizing the routes between cluster nodes might fail.	FW	NGFW-26493
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

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.

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*

© 2020 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
Published 29 April 2020