Forcepoint

Next Generation Firewall

6.10.17

Release Notes

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
- Security enhancements on page 11
- Resolved and known issues on page 11
- Installation instructions on page 12
- Upgrade instructions 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 Long-Term Support (LTS) version.

We recommend using the most recent Long-Term Support (LTS) version if you do not need any features from a later 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.

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 51L)
- 60 Series (N60 and N60L)
- 100 Series (110 and 115) (*Firewall/VPN role only*)
- 120 Series (N120, N120W, N120WL, N120L)
- 320 Series (N321 and N325)
- 330 Series (330, 331, and 335)
- 350 Series (N352 and N355)
- 1000 Series (1035 and 1065)
- 1100 Series (1101 and 1105)
- 1202
- 1402
- 2100 Series (2101 and 2105)
- 2200 Series (2201, 2205, and 2210)
- 3300 Series (3301 and 3305)
- 3400 Series (3401, 3405, and 3410)
- 3500 Series (3510)
- 6205

Note

To use the Forcepoint NGFW Manager, we recommend that you use a Forcepoint NGFW appliance that has at least 4GB of memory.

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

Component	Requirement
Memory	4 GB RAM
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 7.0 ■ KVM with Red Hat Enterprise Linux 7.9 or 8.3 ■ (Firewall/VPN role only) Microsoft Hyper-V on Windows Server 2012 R2 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.

Google cloud, IBM cloud, and Oracle cloud

Forcepoint NGFW 6.10.5 and later versions support public cloud platforms, such as Google, IBM, and Oracle. For more details, see the Knowledge Base Article Knowledge Base article 39116.

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 6.10.17 is 26822.

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

- sg_engine_6.10.17.26822_x86-64-small.iso

```
SHA256SUM:
fa72f5b789e8eda905fee5af18a86bfaeb30da2e6f4b4aa94306cfa4f4b4de16

SHA512SUM:
9b13fb35096fbe82734462ea4e1490fd
ceeecbcabcaf2be0f05cee03600fa151
5ab748e3c5cd0340610d837b0b029d4e
2a8e06e304f876511703406e30a96883
```

- sg_engine_6.10.17.26822_x86-64-small.zip

```
SHA256SUM:
cede9ccab4898dc502fee24474d2555599c50befb53e0f82eaf99c12af91edd1

SHA512SUM:
ca7f43509edc4458cbb984edf845f83a
2ffa84ccfa485c05240518bf1d8e512c
4b01c35a69a187265833bf4df94c0f52
59bb5c3839295eafdf3a55e36fd26ee7
```

Compatibility

Forcepoint NGFW 6.10 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.10 or higher
- Dynamic Update 1337 or higher
- Forcepoint VPN Client 6.6.0 or higher for Windows
- Forcepoint VPN Client 2.0.0 or higher for Mac OS X
- Forcepoint VPN Client 2.0.0 or higher for Android
- Forcepoint VPN Client 2.5.0 or higher for Linux
- Server Pool Monitoring Agent 4.0.0 or higher
- Forcepoint Endpoint Context Agent (ECA) included in Forcepoint One Endpoint 19.05 or higher
- Forcepoint User ID Service 2.0.0 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*, the *Forcepoint Next Generation Firewall Installation Guide*, and the *Forcepoint NGFW Manager and VPN Broker Product Guide*.

External CA issued certificates in internal management communication

Starting with NGFW version 6.10.4, when you install a new SMC, you can now use certificates issued by an external CA instead of certificates generated by the internal CA on the Management Server for internal TLS communication between NGFW Engines and SMC components. Requires NGFW engine version 6.10.4 or newer.

Snort inspection on NGFW Engines

The Snort network intrusion detection system and intrusion prevention system has been integrated into Forcepoint NGFW. You can import externally created Snort configurations into Forcepoint NGFW to use Snort rules for inspection.

You can configure Snort inspection globally for all NGFW Engines, or for individual NGFW Engines. You can use both NGFW deep inspection and Snort inspection for the same traffic, or you can use only NGFW deep inspection or only Snort inspection.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 6.10.17

Enhancement	Description
Support for inspection of Zstandard compressed traffic is added	Inspection process is able to decompress zstd encoded HTTP payload.

Enhancements in Forcepoint NGFW version 6.10.12

Enhancement	Description
Rollback configuration for NGFW Manager	Automatic rollback feature has been added to automatically revert to the previous configuration when management connection to the NGFW Manager or VPN Broker is blocked by the new configuration.

Enhancements in Forcepoint NGFW version 6.10.10

Enhancement	Description
IPv6 small packet performance has been improved.	Packet processing performance has been improved for small IPv6 packets.

Enhancements in Forcepoint NGFW version 6.10.9

Enhancement	Description
Updated Forcepoint NGFW FIPS 140-2 Cryptographic Module	The Forcepoint NGFW FIPS Cryptographic Module used in the FIPS 140-2 mode is updated to version 1.2.1.

Enhancements in Forcepoint NGFW version 6.10.8

Enhancement	Description
Certificate bundle can be imported as VPN Gateway certificate	Prior to NGFW 6.10.8 version, CAs that issue certificates for VPN must be configured in the SMC and included as trusted in both gateway and VPN Profile levels. In later versions, only trust anchor certificates must be configured as trusted. Possible intermediate CAs must be included in the certificate bundle that are being imported as VPN gateway certificate.
Support for bit-based pre-shared keys in IPsec VPN	Bit-based pre-shared keys are entered using a special syntax and are used in IPsec VPN. Specific prefix can be used for hexadecimal and Base64 encoded keys: ■ Any key starting with the prefix "0x" is interpreted as being hexadecimal encoded. ■ Any key starting with the prefix "0s" is interpreted as being Base64 encoded. ■ If neither prefix is identified from the input string the input is assumed to be a plain text key. For more information, see Knowledge Base article 40736 .

Enhancements in Forcepoint NGFW version 6.10.7

Enhancement	Description
SSM SSH Proxy update	The following changes with cryptographic algorithms are available for configuration: ■ Six ciphers removed: `arcfour`, `arcfour128`, `arcfour256`, `blowfish-cbc`, `cast128-cbc`, and `Rijndael-cbc@lysator.liu.se`. ■ Six key exchange algorithms added: `diffie-hellman-group14-sha256`, `diffie-hellman-group16-sha512`, `diffie-hellman-group18-sha512`, `curve25519-sha256`, `curve25519-sha256@libssh.org`, and `sntrup761x25519-sha512@openssh.com`. ■ Three message authentication algorithms removed: `hmac-ripemd160`, `hmac-ripemd160-etm.openssh.com`, and `hmac-ripemd160@openssh.com`. ■ One host key type added: `ssh-ed25519`. **Note** It is recommended to not include the removed algorithms in the policy during NGFW upgrade, as these removed algorithms are stripped from the policy with a warning on Engine upgrade.

Enhancements in Forcepoint NGFW version 6.10.6

Enhancement	Description
Automatic certificate renewal	Automatic certificate renewal lets NGFW Engine to resume communication with the Security Management Center (SMC), where Management Server IP has changed after the previous initial contact had been performed.

Enhancements in Forcepoint NGFW version 6.10.5

Enhancement	Description
Support for ARIA ciphers	TLS decryption now supports ARIA ciphers.
Support for Google Cloud, IBM Cloud, and Oracle Cloud	Forcepoint NGFW 6.10.5 and later versions support public cloud platforms, such as Google, IBM, and Oracle. For more details, see the Knowledge Base Article Knowledge Base article 39116.

Enhancements in Forcepoint NGFW version 6.10.4

Enhancement	Description
Anti-CSRF Tokens for Browser-based authentication	Cross-Site Request Forgery tokens are now available for browser-based authentication templates.

Enhancements in Forcepoint NGFW version 6.10.3

Enhancement	Description
VPN Broker Gateway can help to establish VPN tunnel between two dynamic VPN gateways and VPN Broker Members.	VPN Broker Gateway can notify members behind the NAT about other members trying to contact it. The Broker member behind the NAT initiates connection to members that are trying to contact it.
Detect domain fronting attacks	If HTTP client sent an HTTPS request with mismatching hostname in the TLS SNI extension, then HTTP Host header situation HTTP_Host-SNI-Mismatch is triggered. TLS decryption is required to be able to compare SNI and Host header.
FIPS 140-3 mode can be selected for NGFW Engine.	FIPS 140-3 compatible mode can be enabled in the initial configuration wizard.

Enhancements in Forcepoint NGFW version 6.10.2

Enhancement	Description
Configuration of bidirectional forwarding detection using the Management Client	Forcepoint NGFW Engine previously supported the configuration of bidirectional forwarding detection (BFD) using command line tools on the NGFW Engine. You can now configure BFD using the Management Client. When you use the BGP protocol for dynamic routing, you can optionally use BFD to detect neighbor failures. The NGFW Engine sends packets at the specified interval and waits for a reply. If the NGFW Engine does not receive a reply within the specified length of time, the neighbor is considered to have failed.

Enhancements in Forcepoint NGFW version 6.10.1

Enhancement	Description
TLS inspection for server protection allows TLS handshake downgrade	When you use TLS inspection for server protection without configuring client protection, the certificate authority (CA) can now downgrade unsupported cipher suites, extensions, or ALPN protocols for TLS.
The NGFW Engine skips situation-based matching for encrypted traffic when deep inspection is disabled	The NGFW Engine skips situation-based matching for certain traffic when deep inspection is disabled. When deep inspection and decryption are disabled but the NGFW Engine needs to inspect the beginning of a connection to identify traffic, such as for URL categorization, application identification, or application routing, the NGFW Engine skips situation-based matching later in the connection for certain protocols. Examples of such protocols are TLS and SSH. More protocols may be added via dynamic update packages when deemed suitable. Previously, the NGFW Engine applied situation-based matching and filtered the results.

Enhancements in Forcepoint NGFW version 6.10.0

Enhancement	Description
Improved certificate validation	Certificate validation for TLS inspection and connections from NGFW Engines to external services, such as authentication servers, has been improved. **Note** If you have integrated Forcepoint User ID Service with Forcepoint NGFW, the NGFW Engine can no longer connect to Forcepoint User ID Service servers that use self-signed certificates unless the certificate is explicitly identified with the SHA-1, SHA-256, SHA-512, or MD5 hash of the certificate. To use a self-signed certificate, you must use SHA-1, SHA-256, SHA-512, or MD5 as the TLS Server Identity for the Forcepoint User ID Service element. DNS Name, IP Address, Common Name, and Distinguished Name can no longer be used as the TLS Server Identity for the Forcepoint User ID Service element if you use a self-signed certificate.
SHA-256 support for NTP servers	You can now configure NTP Server elements to use SHA-256 authentication keys.

Security enhancements

For a list of all security enhancements in this product release, see Knowledge Base article 38434.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 38462 .

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*.

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/s/article/Documentation-Featured-Article.

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 6.10 is only supported from version 6.5 or higher. If you have a lower version, first upgrade to version 6.5.

Note

If you use safe search features in NGFW 6.6 or lower, you must refresh the policy on the NGFW Engine cluster after all the members of the cluster have been upgraded to NGFW 6.7 or higher. Otherwise, safe search might not work correctly after the upgrade.

- Forcepoint NGFW version 6.10 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*.

Upgrade notes

- SMC version 6.9 was the last version of the SMC that was compatible with McAfee ePO. Features that depend on McAfee ePO, such as McAfee Threat Intelligence Exchange (TIE) local file reputation sandbox and McAfee® Data Exchange Layer (DXL) local file reputation, are no longer available in SMC 6.10 and higher.

Find product documentation

In the Forcepoint Customer Hub, 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 in the Forcepoint Customer Hub 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 Customer Hub. If you do not yet have credentials, create a customer account. To create a customer account, navigate to the Customer Hub Home page, and then click the **Create Account** link.

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 User Guide*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*
- *Forcepoint NGFW Manager and VPN Broker Product Guide*

© 2025 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 15 April 2025