Next Generation Firewall

6.11.2

Release Notes

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.

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)
- N60
- 100 Series (110 and 115) (*Firewall/VPN role only*)
- 120 Series (N120, N120W, N120WL)
- 330 Series (330, 331, and 335)
- 1100 Series (1101 and 1105)
- 2100 Series (2101 and 2105)
- 2200 Series (2201, 2205, and 2210)
- 3300 Series (3301 and 3305)
- 3400 Series (3401, 3405, and 3410)
- 6205

Note

To use the appliance as VPN Broker or with 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
Memory	4 GB RAM
Hard disk	8GB **Note** RAID controllers are not supported.

Component	Requirement
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
Hypervisor	One of the following: - VMware ESXi 6.5 or 7.0 - KVM with Red Hat Enterprise Linux 7.9 or 8.4 - (Firewall/VPN role only) Microsoft Hyper-V on Windows Server 2012 R2 or Windows Server 2016 with an Intel 64-bit processor

Component	Requirement
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

Starting from Forcepoint NGFW version 6.11 public cloud platforms from Google, IBM, and Oracle are supported. For more details, see the 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 6.11.2 is 27154.

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

- sg_engine_6.11.2.27154_x86-64-small.iso

  ```
  SHA256SUM:

  6b1f93ff8d7dd3f0bc9a4d0fb6b40572d71f3f97490a41b7ea748972a489a8c1

  SHA512SUM:

  7f790552a443f2224b3151a0328422be
  1b335a425c773dcf2afc24ca44095ed8
  951c7f5eea17b56f054123f1f532fadc
  a4000fe6c4db68a5b4353f7d5218d2d5
  ```

- sg_engine_6.11.2.27154_x86-64-small.zip

  ```
  SHA256SUM:

  225340d30b7bf0e45af5d9ae7479ca301fe69d1717eb3cc273e4352e57dec644

  SHA512SUM:

  af373e6337e1af06321c937df8b56e9d
  ec6c3b6016f51117718e9699d9d21a85
  65c068b138746617646a01404416fbfd
  77f896d67fb34af762c976494a5393e3
  ```

Compatibility

Forcepoint NGFW 6.11 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.11 or higher
- Dynamic Update 1423 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

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.

SMC Appliance Restricted Shell

The restricted shell installation option provides improved security on SMC Appliance installations by preventing administrator's direct operating system command line access. Instead, all required administrative tasks are executed through a restricted menu system that only allows access to those commands that are meant for SMC Appliance maintenance.

Run-time selection of FIPS module

In the NGFW Configuration Wizard, you can now select which FIPS module is used when the NGFW Engine is in FIPS-compatible operating mode. You can select whether to use the FIPS 140-2 module or the updated FIPS 140-3 module.

Move Quagga to Free Range Routing (FRR)

The dynamic routing features in the NGFW Engine that previously used the Quagga dynamic routing suite now uses the Free Range Routing (FRR) dynamic routing suite. The Free Range Routing (FRR) is a general purpose routing stack applicable to a wide variety of use cases including connecting hosts, virtual machines, and containers to the network, advertising network services, LAN switching and routing, internet access routers, and Internet peering. If you have manually created dynamic routing configurations on NGFW Engine, you will need to manually verify and convert those to be compatible with new dynamic routing implementation.

Support for TLS 1.3

In addition to the previously supported TLS versions, the NGFW Engine now supports TLS inspection for TLS version 1.3 without downgrading the inspected connections to TLS version 1.2.

IPv6 - IPv4 Translation Support

The NGFW Engine now has basic support for IPv6 transition mechanisms. IPv6 transition mechanisms enable limited communication between devices that have only IPv6 addresses and devices that have only IPv4 address. Supported translation modes are NAT64, 464XLAT, and SIIT EAM.

Upcoming events notification

The upcoming events feature informs users about events that are going to happen soon, such as expiration of licenses and certificates, and failures of scheduled tasks, that require administrator action.

Support TLS server certificate verification before decryption decision

The NGFW Engine now fetches TLS server certificate for verification from destination TLS server with separate probe connection so that it can make a more accurate decision about whether to decrypt TLS connection before the original client to server connection is established.

Status history reporting

The status history provides historical data for monitoring and reporting on NGFW Engines, Netlinks and SD-WAN branch or tunnel statuses over time. New status history views help to visualize past changes in the system status and the traffic and connection volumes and ISP link quality over time. Status monitoring enhancements improve the existing monitoring of SD-WAN branches and VPN tunnels as well as NGFW Engine and Netlink performance history.

Local alternative policies

A local alternative policy can now be defined that can be uploaded but not activated on the NGFW Engine during policy installation. If connectivity between the NGFW Engine and the Management Server is lost, any policy can be selected whether it is a normal policy or one of the local alternative policies.

Deep inspection throughput improved

NGFW detaches deep inspection when it is not needed to improve throughput performance and appliance capacity. This can improve performance for example with encrypted traffic that is not decrypted (e.g. QUIC, SSH, TLS), application identification when further inspection is not needed, and with big file or UDP data steams where NGFW deep inspection is not providing added value.

Support for Google Cloud, IBM Cloud, and Oracle Cloud

Starting from Forcepoint NGFW version 6.11 public cloud platforms from Google, IBM, and Oracle are supported. See Knowledge Base article 39116, for more details.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 6.11

Enhancement	Description
Alternative enhanced SNMP Agent implementation	New SNMP agent can be optionally enabled that replaces the default SNMP Agent. New SNMP Agent supports improved Forcepoint NGFWMIB that provides more monitoring coverage including Virtual NGFW Engines and dynamic routing. In version 6.11 the new agent can be enabled by adding an empty file `/data/config/base/enable_new_snmp` to NGFW Engine file system. For more information, see Knowledge Base article 39118. This now optional enhanced SNMP Agent will be the default SNMP Agent in the next major NGFW Engine release.
VPN Broker configuration usability improvements	Usability of VPN Broker configuration interface has been improved.
Cross Site Request Forgery protection in browser based authentication	Browser Based Authentication now supports Cross Site Request Forgery (CSRF) protection. Protection can be enabled by using new user authentication page template called **User Authentication Pages with CSRF protection**.
DNS name logging	Log columns **DNS Qname**, **DNS Qclass** and **DNS Qtype** can be populated by enabling logging of DNS_Server-Question-Logged and DNS_Record-Address-Logged situations in the inspection policy. See Knowledge Base article 39151 .
Strip H3 HTTP header	When decrypting HTTPS connection for inspection, strip H3 support advertisement from server response in order to prevent HTTP client from switching to HTTP/3. This can be controlled with the new HTTP service parameter Strip QUIC support from server replies. By default this is enabled for HTTPS.
Adjust swap location and size on small NGFW appliances	Follow instructions in the Knowledge Base article 39138 to adjust swap file location on NGFW appliance models.

Enhancements in Forcepoint NGFW version 6.11.1

Enhancement	Description
Support for ARIA ciphers	TLS decryption now supports ARIA ciphers.
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.
Category-based URL filtering can use TLS server certificate information	Server name indication (SNI) is used for URL filtering. If SNI is not used or SNI and server certificate do not match, category-based URL filtering can use domain name from TLS server certificate. For more information, see Knowledge Base article 40739 .

Enhancements in Forcepoint NGFW version 6.11.2

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

Resolved and known issues

This product release contains critical vulnerability fixes. For more details, see Knowledge Base article 41445 . For list of all resolved and known issues in this product release, see Knowledge Base article 39147 .

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 6.11 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 6.11 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*.

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

Published 09 February 2023