



Next Generation Firewall

7.0.1

Release Notes

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 6
- [Enhancements](#) on page 7
- [Resolved and known issues](#) on page 8
- [Security enhancements](#) on page 8
- [Installation instructions](#) on page 8
- [Upgrade instructions](#) on page 9
- [Find product documentation](#) on page 9

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)
- 60 Series (N60 and N60L)
- 120 Series (N120, N120L, N120W, N120WL)
- 330 Series (330, 331, and 335)
- 350 Series (N352 and N355)
- 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® processors based on Westmere microarchitecture or newer.
Memory	4 GB RAM
Hard disk	8GB <div style="margin-top: 10px;">  <p>Note RAID controllers are not supported.</p> </div>

Component	Requirement
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 <p>For information about supported Ethernet interface types and adapters, see Knowledge Base article 9721.</p>

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	<p>One of the following:</p> <ul style="list-style-type: none"> ■ VMware ESXi 6.5 or 7.0 ■ KVM with Red Hat Enterprise Linux 7.9 or 8.5 ■ (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	<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 <p>The following network interface card drivers are recommended:</p> <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.

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 7.0.1 is 28052.

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

- `sg_engine_7.0.1.28052_x86-64-small.iso`

SHA256SUM:

```
a71bb8bc630bf5a99cf4f5ab14ed87dd44f0ed048eb232a782c0510ee94598cb
```

SHA512SUM:

```
b4242d4654053874f5ae406c5d233ea2  
d00d83b630a23defcc1e0420ae2bce86  
e7477af0815e726010b189792bfd5ee8  
ec5bab04f76ec0b2e3af7dc690755f35
```

- `sg_engine_7.0.1.28052_x86-64-small.zip`

SHA256SUM:

```
6ea22fc26dbeb9446570a36a7a4ee2945fab0018149bf49ffb7477629bb8e684
```

SHA512SUM:

```
2678bc80409480908774ccf76e057187  
edcc1c25f18e52771a8b04a148b3fa60  
66d1f49ea836e8fc343902a15880ebb8  
14a2a537bfa4ad3ec316b2c6384ae584
```

Compatibility

Forcepoint NGFW 7.0 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 7.0 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*.

Application health monitoring

The Application Health Monitoring dashboard proactively detects user experience issues based on connection quality metrics. This release introduces a new dashboard and new set of widgets for Application Health Monitoring. For more information, see *Forcepoint Next Generation Firewall Product Guide*.

Integration of ZTNA connector with NGFW Engine

NGFW Engine is typically located in the perimeter of the network where internal resources are located. Therefore, if ZTNA connector is integrated with NGFW Engine, it can be used as a connection point for many services that you might want to publish through FONE portal using the ZTNA connector. From 7.0 onwards, ZTNA connector is integrated with NGFW Engine by default. NGFW hosts a docker container that runs ZTNA connector, which acts as a proxy for FONE portal. For more information about enabling the ZTNA connector, see *Forcepoint Next Generation Firewall Product Guide*. For more information about the ZTNA connector, see *Zero Trust Network Access* section in *Forcepoint ONE Admin Guide*.

Web filtering and Network Application detection for QUIC

Web filtering and Network Application detection for QUIC is targeted for users who are using inspection features such as Network and URL applications but are not decrypting the traffic.

QUIC protocol is always inspected and by default matched for web traffic rules. In this release, decryption of QUIC traffic is not supported but discarding the QUIC traffic causes most of the standard web clients fall back to earlier versions of HTTP, for which decryption by TLS inspection is supported. For more information about this feature, see *Forcepoint Next Generation Firewall Product Guide*.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 7.0

Enhancement	Description
Action options are now configurable in the Inspection Situation Tree	Action options can now be configured for situations directly in the inspection policy's Inspection tab where the global inspection situation tree with Permit and Terminate actions are configured.
Re-factor and optimize dynamic DNS matching	DNS based rule matching has been enhanced to optimize the rule matching speed.
Blacklist and Whitelist terminologies are not used in customer views	The old terminologies "Blacklist" and "Whitelist" are replaced with "Block List" and "Allow List" respectively.
Enhanced version of the SNMP Agent used by default in NGFW Engine version 7.0	When upgrading to NGFW 7.0, with SNMP Agent enabled in configuration, NGFW engine automatically switches to enhanced SNMP Agent. For more information, see Knowledge Base article 41106 .

Enhancement	Description
4096 bit RSA key support for Browser Based User Authentication (BBA)	Browser Based User Authentication (BBA) HTTPS settings now support generating 4096 bit RSA key certificate request for the BBA server component.
IPv6 small packet performance has been improved.	Packet processing performance has been improved for small IPv6 packets.
Policy changes are installed faster for remote NGFW Engines	With policy refresh only files with configuration changes are uploaded to the NGFW Engine. Rules alone are now stored on their own configuration file reducing amount of data to be uploaded to NGFW Engine with just a policy change. As result policy refresh for remote engines behind slow throughput Internet connection is faster.

Enhancements in Forcepoint NGFW version 7.0.1

Enhancement	Description
TLS inspection support for SMTP using opportunistic TLS	SMTP connections using opportunistic TLS (STARTTLS) can now be decrypted and inspected.
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.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article [41215](#) .

Security enhancements

This product release contains critical vulnerability fixes. For more details, see Knowledge Base article [41445](#) . For list of all security enhancements in this product release, see Knowledge Base article [41217](#) .

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 7.0 is only supported from version 6.8 or higher. If you have a lower version, first upgrade to version 6.8.

- Forcepoint NGFW version 7.0 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*

