



# Next Generation Firewall

6.8.2

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 7
- [Enhancements](#) on page 8
- [Resolved issues](#) on page 9
- [Installation instructions](#) on page 10
- [Upgrade instructions](#) on page 11
- [Known issues](#) on page 12
- [Find product documentation](#) on page 12

# 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.



## 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*)
- 120W
- 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




## 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
Memory	4 GB RAM
Hard disk	8GB  <b>Note</b> RAID controllers are not supported.
Peripherals	<ul style="list-style-type: none"> <li>■ DVD drive</li> <li>■ VGA-compatible display</li> <li>■ Keyboard</li> </ul>
Interfaces	<ul style="list-style-type: none"> <li>■ One or more network interfaces for the Firewall/VPN role</li> <li>■ Two or more network interfaces for the IPS in IDS configuration</li> <li>■ Three or more network interfaces for inline IPS engine or Layer 2 Firewall</li> </ul> For information about supported Ethernet interface types and adapters, see Knowledge Base article <a href="#">9721</a> .

# 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: <ul style="list-style-type: none"> <li>VMware ESXi 6.5 or 6.7</li> <li>KVM with Red Hat Enterprise Linux 7.8 or 8.1</li> <li>(Firewall/VPN role only) Microsoft Hyper-V on Windows Server 2012 R2 or Windows Server 2016 with an Intel 64-bit processor</li> </ul>
Interfaces	<ul style="list-style-type: none"> <li>At least one virtual network interface for the Firewall/VPN role</li> <li>Three virtual network interfaces for IPS or Layer 2 Firewall roles</li> </ul> <p>The following network interface card drivers are recommended:</p> <ul style="list-style-type: none"> <li>VMware ESXi platform — <code>vmxnet3</code>.</li> <li>KVM platform — <code>virtio_net</code>.</li> </ul>

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 6.8.2 is 24155.

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

- `sg_engine_6.8.2.24155_x86-64-small.iso`

```
SHA1SUM:  
ad7328bc34b26eea25e8ba31f15bdd914235fdb9  
  
SHA256SUM:  
0b77619cdd72c2bcc40818228ad243b0f8b9a441b3d4aeec9911ccd9d0476d34  
  
SHA512SUM:  
7c563b36436e876d5e802dd10849271f  
dad054510d9cace2b30a99a80ed2a162  
959b1327387cf0699f451917ae934712  
78a104225a7a306ecb4b55815444f61f
```

- `sg_engine_6.8.2.24155_x86-64-small.zip`

```
SHA1SUM:  
5ac88544e8fae43f612c84767d23ddc7c35f40ea  
  
SHA256SUM:  
d44cfd37472aa97f84147ffeab85890b2a5dedcf5bcb37669c3926b9d5c0d46c  
  
SHA512SUM:  
d85344f41157c03491a0f0db61425533  
e9387af457d694ffa77f4e23c9a3672b  
f144fc89fb63e88787adc7df653dd6cb  
4024db8abd75a524f73cdc6e53c5cafb
```

## Compatibility

Forcepoint NGFW 6.8 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.8 or higher
- Dynamic Update 1247 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) 1.4.0 or higher
- Forcepoint Endpoint Context Agent (ECA) included in Forcepoint One Endpoint 19.05 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*.

### Easier configuration of dynamic link selection for NGFW Engines

---

It is now possible to select Link Usage Profile elements for NGFW Engines in the Firewall/VPN role to define which link types are preferred, avoided, or not used for specific types of outbound Multi-Link traffic. NGFW Engine-specific exceptions to the Link Usage Profile also allow you to specify which traffic uses specific NetLinks.

### PPPoE support on VLAN interfaces

---

You can now configure point-to-point protocol over Ethernet (PPPoE) for dynamic IP addresses that are assigned to VLAN interfaces. Using PPPoE for dynamic IP addresses that are assigned to VLAN interfaces allows you to connect to an ISP line that uses 802.1q VLAN tagging without using a separate switch.

### Re-authentication when using browser-based user authentication

---

If an end user has authenticated using browser-based user authentication and the session will soon expire, the user can re-authenticate to extend the authentication time-out and avoid connections closing before the user has finished their tasks.

### Dynamic update packages in the NGFW Manager

---

You can now upload and activate dynamic update packages in the NGFW Manager. Dynamic update packages provide updates for NGFW Engines, especially for deep inspection features.

For example, new threat patterns and changes in the system Templates and Policies are introduced in dynamic updates for up-to-date detection. They can also revise the default elements you use to configure the system.

For more information, see the *Forcepoint NGFW Manager and VPN Broker Product Guide*.

### Support for the NGFW Engine tester in the NGFW Manager

---

You can now use the NGFW Engine tester in the NGFW Manager. The NGFW Engine tester runs various checks on the NGFW Engine and initiates responses based on the success or failure of these tests.

For more information, see the *Forcepoint NGFW Manager and VPN Broker Product Guide*.

## Enhancements

This release of the product includes these enhancements.

### Enhancements in Forcepoint NGFW version 6.8.0

Enhancement	Description
Custom script upload for NGFW Engines when using Custom Properties Profile elements	To upload custom scripts to the NGFW Engine, you can add the scripts to the properties of the NGFW Engine using a Custom Properties Profile element. The scripts are uploaded when the policy is installed or refreshed.
Expiration time for one-time passwords	You can now set the expiration time for one-time passwords that are generated when you save the initial configuration for an NGFW Engine. If the one-time password is not used, it automatically expires after the expiration time has elapsed. By default, one-time passwords expire after 30 days.
User domain support for integrated ICAP servers for DLP	NGFW integration with external ICAP servers for DLP now uses the WinNT schema in the X-Authenticated-Users header instead of the Local schema that was used previously. Using the WinNT schema allows matching users against a user domain in the user directory on the ICAP server.
Significant improvements in inspection performance	There are general improvements in how the NGFW Engines inspect traffic. Inspection performance has improved significantly, especially when application detection is enabled.
VPN broker member synchronization in VPN Broker high availability environment	When you use the VPN Broker in a high availability (HA) environment, the changes you make to the list of VPN Broker members are automatically synchronized with all the other VPN Broker gateways in the NGFW Manager.
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.

### Enhancements in Forcepoint NGFW version 6.8.1

Enhancement	Description
Improved VPN performance	VPN performance has been improved in environments where there is a high rate of new VPN connections.



# 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.

The **Role** column indicates the NGFW Engine roles that are affected by the issue:

- FW — Firewall/VPN
- IPS — IPS
- L2FW — Layer 2 Firewall
- VPN Broker — VPN Broker gateway

To resolve the issue, upgrade NGFW Engines that have the specified roles.

Description	Role	Issue number
Traffic that is received through a VPN might experience packet loss.	FW, VPN Broker	NGFW-23700
The session and certificate caches for TLS decryption might not clear old entries effectively.	FW, IPS, L2FW	NGFW-26704
When credentials for TLS decryption have been configured but decryption is disabled for the connection, TLS 1.3 connections might be terminated with the TLS_Unrecoverable-Error situation.	FW, IPS, L2FW	NGFW-27016
When QoS is applied to traffic, counters for packets transmitted do not show traffic on tunnel interfaces.	FW	NGFW-27272
In rare cases, the VPN process might restart during IKE negotiation.	FW, VPN Broker	NGFW-27284
When the NGFW Engine is handling SIP UDP traffic, the inspection process might restart.	FW, IPS, L2FW	NGFW-27725
NGFW appliance models 110 and 115 might have too little free memory available for policy installation.	FW, IPS, L2FW	NGFW-27921
In rare cases when the security association granularity for VPN negotiation is SA per Host, the VPN process might fail to handle the negotiation and cause the NGFW Engine to restart.	FW, VPN Broker	NGFW-28249
Master NGFW Engines that only have a single node might send out some packets using the state synchronization multicast IP address.	FW, IPS, L2FW	NGFW-28251
User responses might show the incorrect URL category for blocked URLs in HTTP/2 traffic.	FW, IPS, L2FW	NGFW-28292
When you use application routing, the TLS handshake might be delayed if the NGFW Engine cannot identify the application based on the TLS Client Hello packet.	FW	NGFW-28379
The "Any Network" element and overlapping networks on VPN Broker Members might not be handled correctly.	FW, VPN Broker	NGFW-28381
When the access rules include some specific custom elements, such as Network Application and URL List elements, policy installation might fail due to internal consistency checks.	FW, IPS, L2FW	NGFW-28383
SNMP monitoring for VPN SAs always returns 0 as the value.	FW	NGFW-28392

Description	Role	Issue number
The inspection process might restart if application routing is used.	FW	NGFW-28405
When GTI has been enabled but the NGFW Engine does not have a default route or a proxy configured for connections to the Internet, the inspection process might restart.	FW, IPS, L2FW	NGFW-28506
When inspection is enabled, file uploads using HTTP/2 might fail.	FW, IPS, L2FW	NGFW-28509
In a VPN Broker configuration, the antispoofing configuration is not always correctly generated for the networks of VPN Broker Members. Networks that have both IPv4 and IPv6 addresses are also not handled correctly in routing.	FW	NGFW-28514
In rare cases, the node might go offline because dynamic routing uses too much memory.	FW	NGFW-28542
When the NGFW Engine initiates reset packets for traffic that uses a VPN, the NGFW Engine might not correctly send the reset packets.	FW	NGFW-28595
When you use the ratio-based load-balancing method for outbound Multi-Link, monitoring views in the Management Client do not show the number of concurrent connections that are currently using the outbound Multi-Link.	FW	NGFW-28718
When you modify a large VPN configuration, policy installation might take too long and the VPN process might restart.	FW	NGFW-28887
ICMP ID is used to monitor external VPN endpoints. If you use load balancing clustering, ICMP echo replies from remote endpoints might be discarded.	FW	NGFW-28940
When deep inspection closes a connection due to memory deallocation, the reason is not indicated in the connection closed log message.	FW, IPS, L2FW	NGFW-28946
When traffic is allowed using Network Application elements, application routing might not work correctly for TLS traffic that does not include an SNI (Server Name Indication).	FW	NGFW-29005

## 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 6.8 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 6.8 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*.

# Known issues

For a list of known issues in this product release, see Knowledge Base article [18382](#).

## 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, release notes, 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 User Guide*
- *Forcepoint VPN Client User Guide for Windows or Mac*
- *Forcepoint VPN Client Product Guide*

