



# Next Generation Firewall

6.8.7

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 11
- [Upgrade instructions](#) on page 12
- [Known issues](#) 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.



## 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> <p>For information about supported Ethernet interface types and adapters, see Knowledge Base article <a href="#">9721</a>.</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	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 6.8.7 is 24405.

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

- `sg_engine_6.8.7.24405_x86-64-small.iso`

```
SHA1SUM:  
15b9ed8d87136dc2527a9f8464e3a503e94bfb5a  
  
SHA256SUM:  
096c5fc4f023f646d139e0b77b1130c2a3cfe4f52fd679d733de0086b8b9fa5e  
  
SHA512SUM:  
9fa87c4ff644e0b03fb94185abb971fa  
970e3617cfd1561c8f2bdcd485beb4ee  
99389a647fc616b93a14310a2dca4a07  
ba24bd0b0c55f6ddca64a59ba2488281
```

- `sg_engine_6.8.7.24405_x86-64-small.zip`

```
SHA1SUM:  
8e2614ced9df7c3d754b15aefd851c394236ef76  
  
SHA256SUM:  
76cf35992994596e3a9f57f87b1afc1747efd737b48ca8769c5ca6c5d6e7acfa  
  
SHA512SUM:  
af5d1ba63c8b61baed13756f0e3f1f0f  
eb47174b8a196e7f739bc6c0df11d96d  
2dbc1a134ba11a81c196e1c87765743c  
7029083b60f11ddf393da1908b56c79e
```

## 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.



## Enhancements in Forcepoint NGFW version 6.8.4

Enhancement	Description
More memory usage details available using SNMP Agents for NGFW Engines	Two new counters for available memory are now reported in Forcepoint NGFW-specific SNMP MIBs. The new OIDs are fwMemBytesAvailable and fwMemBytesSReclaimable. To use the new counters, update the NGFW-specific SNMP MIB for your SNMP tools to the NGFW MIB 6.9 level. For more information, see Knowledge Base article <a href="#">19210</a> .

## Enhancements in Forcepoint NGFW version 6.8.5

Enhancement	Description
Detections of brute force attacks against NGFW user authentication	After you install dynamic update package 1303 or higher, you can use new Correlation Situation elements to detect and prevent brute force attacks against NGFW user authentication. For more information, see Knowledge Base article <a href="#">19259</a> .

## Enhancements in Forcepoint NGFW version 6.8.6

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.
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.
Improved performance of interface driver for virtualization platforms	The performance of the vmxnet3 interface driver for virtualization platforms has been improved.

## 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
When the dynamic IP address of an interface changes or a new interface with a dynamic IP address is added, the process related to wireless interfaces is restarted. As a result, hosts that are connected using WLAN must reconnect.	FW	NGFW-26496
When there is a large number of spooled log entries, the rate at which the NGFW Engine is able to send log data to the Log Server decreases significantly. As a result, it can take longer than expected to send all the spooled log entries to the Log Server even though the log connection is well established.	FW, IPS, L2FW	NGFW-30479
When you use protocol identification, the NGFW Engine might hold the first packets of connections from some protocols, such as telnet or speed test applications, where the first message is very short. As a result, the connection seems to stop progressing.	FW, IPS, L2FW	NGFW-32453
Some TCP keep alive packets might trigger the TCP_Segment-Content-Conflict situation.	FW, IPS, L2FW	NGFW-32785
Alerts triggered by packet validity situations do not have a severity. Alerts without a severity do not match if severity is used as matching criteria in the Alert Policy.	FW, IPS, L2FW	NGFW-32958
The NGFW Engine informs other devices in the network of MAC address changes using gratuitous ARP packets. On interfaces that are shared by multiple Virtual NGFW Engines, gratuitous ARP packets are not sent correctly.	FW	NGFW-33459
When there is already a dynamic route to the same destination, static IPv6 routes are not added to the routing configuration correctly.	FW	NGFW-33567
When you use the VPN Broker, a VPN Broker Member that has endpoints with dynamic IP addresses might incorrectly send APIPA addresses to the VPN Broker Gateway. As a result, other VPN Broker Members cannot contact the VPN Broker Member.	FW	NGFW-33897
DNS resolution might stop working on Master NGFW Engine nodes.	FW, IPS, L2FW	NGFW-34061
TACACS+ authentication fails.	FW	NGFW-34440
When you use NAT rules for application routing, NGFW Engine nodes might restart.	FW	NGFW-34446
In rare cases, the VPN process might restart.	FW	NGFW-34460
In some specific configurations, the memory usage for the inspection process might increase over time.	FW, IPS, L2FW	NGFW-34480
If you use SunRPC services in Layer 2 Access rules, the NGFW Engine might not operate normally.	FW	NGFW-34515
When the value of the Default Connection Termination in Inspection Policy option is Only Log Connection, Access rules that should terminate the connection and trigger a User Response only create a Terminate (passive) log entry without stopping the matching connections.	FW, IPS, L2FW	NGFW-34539
When VPNs are configured, policy installation might fail during policy validation.	FW	NGFW-34547
In rare cases, when inspection is enabled, the NGFW Engine might restart when you install a policy.	FW, IPS, L2FW	NGFW-34553
When endpoint applications are configured and many connections are repeated around the same time, the inspection process might restart.	FW, IPS, L2FW	NGFW-34603

Description	Role	Issue number
If traffic arrives at a Virtual NGFW Engine interface at the same moment that the interface is removed during policy installation, the NGFW Engine might restart.	FW, IPS, L2FW	NGFW-34694
If a device sends an SDP media descriptor without format specifiers, SDP parsing fails. As a result, when you release a SIP call from hold, the call might fail.	FW, IPS, L2FW	NGFW-34734
If you remove the VPN Broker configuration from a Firewall Cluster and reboot one of the nodes, the rebooted node might remain in the offline state.	FW	NGFW-34747
SNMP monitoring for uptime might return the wrong time when the uptime is over 248 days.	FW, IPS, L2FW	NGFW-34765
When you use zones as matching criteria in Access rules, connections might be incorrectly closed after policy installation. The following message is show in the log entries: "Connection was discarded by new policy".	FW	NGFW-34787
If you change the RX/TX ring descriptor count for an interface that uses the ixgbe, i40e, or ice driver on the command line, the NGFW Engine might restart.	FW, IPS, L2FW	NGFW-34819
When there is a very large VPN configuration, some of the IPsec tunnels might be renegotiated when you install a policy on the NGFW Engine. As a result, VPN traffic might be briefly interrupted.	FW	NGFW-34834
When you use route metrics to select the route for dynamic routing and you have configured a static route with a higher metric value, the NGFW Engine might not use routes with lower metric values learned from dynamic routing.	FW	NGFW-35128

## 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>.

### 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

---

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 Reference Guide*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*

