



# **FORCEPOINT**

## **Next Generation Firewall**

**Release Notes**

**6.2.1**

**Revision A**

## Contents

- [About this release](#) on page 2
- [Lifecycle model](#) on page 2
- [System requirements](#) on page 3
- [Build version](#) on page 6
- [Compatibility](#) on page 7
- [New features](#) on page 7
- [Enhancements](#) on page 9
- [Resolved issues](#) on page 9
- [Installation 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); formerly known as Stonesoft® Next Generation Firewall by Forcepoint (Stonesoft 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 later Feature Stream version.

For more information about the Forcepoint NGFW lifecycle policy, see Knowledge Base article [10192](#).

# System requirements

Make sure that you meet these basic hardware and software requirements.

## Forcepoint NGFW appliances

We strongly recommend using a pre-installed Forcepoint NGFW appliance as the hardware solution for new Forcepoint NGFW installations.



**Note:** Some features in this release are not available for all appliance models. See Knowledge Base article [9743](#) for up-to-date appliance-specific software compatibility information.

Two Forcepoint NGFW engine images are available:

- x86-64 — A 64-bit image that includes the Local Manager.
- x86-64-small — A 64-bit image that does not include the Local Manager.



**Note:** If you do not use the Local Manager, we recommend that you use the x86-64-small image. Some appliance models support only the x86-64-small image.

The following table shows whether you can use an appliance model in the Firewall/VPN (FW), IPS, or Layer 2 Firewall (L2FW) role, and the image that is supported.

| Appliance model | Roles         | Images   |
|-----------------|---------------|--|
| FW-315          | FW            | The image that does not include the Local Manager is supported |
| 320X (MIL-320)  | FW            | Both images are supported                                      |
| IPS-1205        | IPS, L2FW     | Both images are supported                                      |
| FWL321          | FW            | The image that does not include the Local Manager is supported |
| NGF321          | FW, IPS, L2FW | Both images are supported                                      |
| FWL325          | FW            | The image that does not include the Local Manager is supported |
| NGF325          | FW, IPS, L2FW | Both images are supported                                      |
| 110             | FW            | The image that does not include the Local Manager is supported |
| 115             | FW            | The image that does not include the Local Manager is supported |
| 1035            | FW, IPS, L2FW | Both images are supported                                      |
| 1065            | FW, IPS, L2FW | Both images are supported                                      |
| 1301            | FW, IPS, L2FW | Both images are supported                                      |
| 1302            | FW, IPS, L2FW | Both images are supported                                      |
| 1401            | FW, IPS, L2FW | Both images are supported                                      |
| 1402            | FW, IPS, L2FW | Both images are supported                                      |
| 3201            | FW, IPS, L2FW | Both images are supported                                      |

| Appliance model | Roles         | Images                    |
|-----------------|---------------|---------------------------|
| 3202            | FW, IPS, L2FW | Both images are supported |
| 3205            | FW, IPS, L2FW | Both images are supported |
| 3206            | FW, IPS, L2FW | Both images are supported |
| 3207            | FW, IPS, L2FW | Both images are supported |
| 3301            | FW, IPS, L2FW | Both images are supported |
| 3305            | FW, IPS, L2FW | Both images are supported |
| 5201            | FW, IPS, L2FW | Both images are supported |
| 5205            | FW, IPS, L2FW | Both images are supported |
| 5206            | FW, IPS, L2FW | Both images are supported |

## Sidewinder S-series appliances

These Sidewinder appliance models can be re-imaged to run Forcepoint NGFW software.

| Appliance model | Roles | Images                    |
|-----------------|-------|---------------------------|
| S-1104          | FW    | Both images are supported |
| S-2008          | FW    | Both images are supported |
| S-3008          | FW    | Both images are supported |
| S-4016          | FW    | Both images are supported |
| S-5032          | FW    | Both images are supported |
| S-6032          | FW    | Both images are supported |

## Certified Intel platforms

We have certified specific Intel-based platforms for Forcepoint NGFW.

The tested platforms can be found at <https://support.forcepoint.com> under the Forcepoint Next Generation Firewall product.

We strongly recommend using certified hardware or a pre-installed Forcepoint NGFW appliance as the hardware solution for new Forcepoint NGFW installations. If it is not possible to use a certified platform, Forcepoint NGFW can also run on standard Intel-based hardware that fulfills the hardware requirements.

## Basic hardware requirements

You can install Forcepoint NGFW on standard hardware with these basic requirements.

- (Recommended for new deployments) Intel® Xeon®-based hardware from the E5-16xx product family or higher



**Note:** Legacy deployments with Intel® Core™2 are supported.

- IDE hard disk and DVD drive



**Note:** IDE RAID controllers are not supported.

- Memory:
  - 4 GB RAM minimum for x86-64-small installation
  - 8 GB RAM minimum for x86-64 installation
- VGA-compatible display and keyboard
- One or more certified network interfaces for the Firewall/VPN role
- Two or more certified network interfaces for IPS with IDS configuration
- Three or more certified network interfaces for Inline IPS or Layer 2 Firewall

For information about certified network interfaces, 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 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.

- (Recommended for new deployments) Intel® Xeon®-based hardware from the E5-16xx product family or higher



**Note:** Legacy deployments with Intel® Core™2 are supported.

- One of the following hypervisors:
  - VMware ESXi 6.1 and 6.5
  - KVM (KVM is tested as shipped with Red Hat Enterprise Linux Server 7.1 and 7.2)
- 8 GB virtual disk
- 4 GB RAM minimum

- A minimum of one virtual network interface for the Firewall/VPN role, three for IPS or Layer 2 Firewall roles
- 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.

## Build version

Forcepoint NGFW 6.2.1 build version is 18054.

## Product binary checksums

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

- **sg\_engine\_6.2.1.18054\_x86-64.iso**

```
SHA1SUM:
3ed346e9c91f04215d294c659ddae40041fa3b71

SHA256SUM:
063bec31de492ed024410e50a459f576649dbce0a5a92aac538cb512fd8623f9

SHA512SUM:
51b4571d749012eb40ba3b1bf95e871c
3755ac65c4d27e60b9c80c806d384297
94bbb23c08ea298faac95ec0af09ecc4
a03409e3e791d8edce7d05770aa21ad3
```

- **sg\_engine\_6.2.1.18054\_x86-64.zip**

```
SHA1SUM:
a06e8a7e3008fd562960abd09dee7d6b0dd7d746

SHA256SUM:
0ce283d13905017dd672bbf53cd43da330a8694921e53062fed64a0f69ebc604

SHA512SUM:
8b6a76c90c69dc806164307f6acace78
9cbb237a48ecd53086c96b29ce987b4f
1ff9ea284dc95dde440e6275f8bc8d07
509b47f01c81d24d69f614e3127a9692
```

- **sg\_engine\_6.2.1.18054\_x86-64-small.iso**

```
SHA1SUM:
f6a8a005521fe87acad6445bcc83fbd1dac65905

SHA256SUM:
9ce2d052584146b50e112c8fa03e9e7478381ff6f03ea1b5bbce9a9961978c14

SHA512SUM:
57a3a273f62dec2e09f149ad8ec5c09
645d1fd13f2522e46eb272ec21b9bfbf
6a1d591f9b6af2e0385eec5fa161456a
dbd78a72d95f5b8556dafa41663219a7
```

- `sg_engine_6.2.1.18054_x86-64-small.zip`

```
SHA1SUM:
3961137863922a949ea69e7fdbf4f5357d54e5d2

SHA256SUM:
6cba93a282e6b7dd4783031ff7aef5c06569256bf80f198cf8ee0c83f15ad688

SHA512SUM:
f58b1d5203855eb79d71a3147ad1e360
ed5a20c7a65e20252a227cbc678ecc65
ced7bfb758ac23a69a55b840f45c5460
3427f05ebfb2fb824da0e44f05d89ce4
```

## Compatibility

---

Forcepoint NGFW 6.2 is compatible with the following component versions.

- Forcepoint™ NGFW Security Management Center (SMC) 6.2 or later
- Dynamic Update 864 or later
- Stonesoft® VPN Client for Windows 6.0.0 or later
- Stonesoft® VPN Client for Mac OS X 2.0.0 or later
- Stonesoft® VPN Client for Android 2.0.0 or later
- Server Pool Monitoring Agent 4.0.0 or later
- McAfee® Logon Collector 2.2 and 3.0
- McAfee® Advanced Threat Defense 3.6
- McAfee® Endpoint Intelligence Agent (McAfee EIA) 2.5

## 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*.

### Forcepoint Advanced Malware Detection

---

Forcepoint Advanced Malware Detection uses file reputation scans in a sandbox service to detect advanced threats. The Cloud Sandbox analyzes the behavior of files in a restricted operating system environment and returns a reputation score for the files. From the Logs view of the Management Client, you can access an external portal where you can view detailed reports for files that have been analyzed in the Cloud Sandbox. You can also use analysis and reporting tools in the external portal.



**Note:** Forcepoint Advanced Malware Detection requires a separate license for the Cloud Sandbox service. See Knowledge Base article [12514](#).

## Pending configuration changes shown for NGFW Engines

---

You can now view configuration changes that you and other administrators have made before the new configurations are transferred to the engines. The pending changes are shown in the Home view and on the selected engine's home page. You can optionally also enforce an approval workflow. When an approval workflow is enforced, administrators with unrestricted permissions must approve all pending changes before the changes can be committed.

## Support for Sidewinder Proxies on Virtual NGFW Engines in the Firewall/VPN role

---

You can now use Sidewinder Proxies (HTTP, SSH, TCP, and UDP) on Virtual NGFW Engines in the Firewall/VPN role. Sidewinder Proxies on Forcepoint NGFW enforce protocol validation and restrict the allowed parameters for each protocol. Sidewinder Proxies are primarily intended for users in high assurance environments, such as government or financial institutions. In environments that limit access to external networks or access between networks with different security requirements, you can use Sidewinder Proxies for data loss protection.

## DNS Relay on NGFW Engines in Firewall/VPN role

---

DNS relay allows NGFW Engines in the Firewall/VPN role to provide DNS services for internal networks. The firewall forwards DNS requests from clients in the internal network to remote DNS servers and temporarily stores the results of the DNS requests in the cache. The firewall can forward DNS requests to different DNS servers depending on the domain in the DNS request. The firewall can also return fixed DNS results for specific hosts or domains, and translate external IP addresses in DNS replies to IP addresses in the internal network.

## Improved dynamic multicast routing support on NGFW Engines in Firewall/VPN role

---

You can now configure protocol-independent multicast (PIM) on NGFW Engines in the Firewall/VPN role in the Management Client. Previously, you could only configure PIM on the engine command line. You can use source-specific multicast (PIM-SSM), sparse mode (PIM-SM), or dense mode (PIM-DM).

## Improved logging and diagnostics for SSL VPN Portal

---

Logging and diagnostics have been improved for the SSL VPN Portal. Log entries are generated when an SSL VPN Portal user starts and ends a session. If diagnostics are enabled for the SSL VPN Portal, log entries are also generated for HTTP or HTTPS transactions. SSL VPN Portal users can see the time of their last logon and the number of failed logon attempts in the status bar of the SSL VPN Portal.



# Enhancements

This release of the product includes these enhancements.

## Enhancements in Forcepoint NGFW version 6.2.0

| Enhancement                              | Description  |
|--|--|
| NetLink-specific DNS IP addresses        | You can now define NetLink-specific DNS IP addresses for static NetLinks. Dynamic NetLinks can automatically learn DNS IP addresses.   |
| Improved configuration of User Responses | User Responses are now easier to configure. The new message response allows you to quickly create simple messages without using HTML markup. You can also use variables in User Responses to provide connection-specific information to the end users. |

## Enhancements in Forcepoint NGFW version 6.2.1

| Enhancement  | Description  |
|--|--|
| Improved scaling of dynamic routing for Virtual NGFW Engines | Dynamic routing now scales up better with a large number of Virtual NGFW Engines.  |
| Cloud Sandbox logging has been enhanced                      | <p>A file allowed through an NGFW Engine and later found out to be malicious previously created only a "File reputation updated" log entry. Now also a log entry with the "File_Malware-Detected" Situation is displayed.</p> <p>SMC logs did not previously indicate that unsupported file types were sent to the Cloud Sandbox for inspection. Now "Sandbox_Unsupported-File-Type" Situations are logged when an unsupported file type has been sent to the Cloud Sandbox.</p> |

# Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in earlier releases, see the Release Notes for the specific release.

| Description   | Role          | Issue number |
|---|---------------|--------------|
| If multiple HTTP proxy servers are defined for GTI file reputation, ThreatSeeker, or the Cloud Sandbox in the Engine Editor, the engine uses only one of the servers.               | FW, IPS, L2FW | NGFW-1455    |
| When you take traffic captures using the Management Client, transferring the traffic captures from the engine to the SMC might fail. The CPU load on the engine might also be high. | FW, IPS, L2FW | NGFW-3576    |

| Description  | Role          | Issue number |
|--|---------------|--------------|
| Connections through a cluster in load-balancing mode might have a high latency if they go through an Aggregated Link interface or an interface that uses VLANs.  | FW            | NGFW-3740    |
| After refreshing the policy, misleading state synchronization log entries about lost state synchronization packets might be displayed.   | FW, IPS, L2FW | NGFW-3930    |
| The engine might become unresponsive or stop working if the appliance has a large number of CPU cores and there are a large number of new concurrent connections in the VPN.   | FW            | NGFW-3981    |
| File reputation might not be received from the Cloud Sandbox if the Cloud Sandbox service is disabled in the Management Client and then enabled again without rebooting the NGFW Engine after disabling the service.           | FW, IPS, L2FW | NGFW-4166    |
| When the VPN Gateway to which VPN Clients connect is a Virtual NGFW Engine, VPN Client users might not be able to re-authenticate.   | FW            | NGFW-4212    |
| Server Pool failover to the remaining Server Pool members might not work with connections that do not use TCP.   | FW            | NGFW-4295    |
| When you create the first Virtual NGFW Engine for a Master NGFW Engine, the first policy installation after the Virtual NGFW Engine has been created might fail. After about half an hour, policy installation works normally. | FW, IPS, L2FW | NGFW-4326    |
| When the NGFW Engine receives a large number of Users and User Groups, for example from McAfee Logon Collector, the NGFW Engine might process traffic more slowly.   | FW, IPS, L2FW | NGFW-4327    |
| On interfaces that use the MOE10F4 (MOD-EM2-10G-SFP-4) or MO40F2 (MOD-40G-2) interface modules, link aggregation might stop working when you change the number of VLAN Interfaces on an Aggregated Link interface.             | FW            | NGFW-4419    |
| When you change the interface configuration on an NGFW Engine that has a large number of Physical Interfaces or VLAN Interfaces, policy installation can temporarily interrupt the flow of traffic.                            | FW            | NGFW-4420    |
| If the engine has a large number of Physical Interfaces and VLAN Interfaces, status monitoring might periodically report the engine as unreachable.  | FW            | NGFW-4433    |
| The use of the Cloud Sandbox service might cause high memory usage spikes.   | FW, IPS, L2FW | NGFW-4490    |
| When an NGFW Engine in the IPS role inspects connections picked up through a Capture Interface, memory consumption might become unusually high.  | IPS           | NGFW-4497    |
| If the Quality of Service (QoS) mode "QoS Statistics Only" is configured for some interfaces while other interfaces use other QoS modes, the engine might stop processing traffic.   | FW, IPS, L2FW | NGFW-4551    |
| The McAfee anti-malware version used by NGFW has been upgraded to address CVE-2016-8031.   | FW, IPS, L2FW | NGFW-4730    |
| On engines that have 300 or more Physical Interfaces or VLAN Interfaces, Aggregated Link Interfaces might not work correctly.  | FW            | NGFW-4733    |

| Description   | Role          | Issue number |
|---|---------------|--------------|
| The throughput for license-based throughput limit might be calculated higher than it actually is.   | FW            | NGFW-4885    |
| Querying the reputation of a file previously inspected by the Cloud Sandbox might not provide a reputation. The file might be sent again to the Cloud Sandbox for inspection. | FW, IPS, L2FW | NGFW-5002    |

## Installation instructions

Use these high-level steps to install 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>.



**Note:** The sgadmin user is reserved for SMC use on Linux, so it must not exist before SMC is installed for the first time.

### 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 with the Management Client using the **Configuration** view.
- 4) To generate initial configurations for the engines, right-click each Firewall, IPS, or Layer 2 Firewall element, then select **Configuration > Save Initial Configuration**.  
Make a note of the one-time password.
- 5) Make the initial connection from the engines to the Management Server, then enter the one-time password.
- 6) Create and upload a policy on the engines using the Management Client.

## Upgrade instructions

Take the following into consideration before upgrading licenses, engines, and clusters.

- Upgrading to version 6.2 is only supported from version 5.10 or later. If you have an earlier version, first upgrade to version 5.10.
- Forcepoint NGFW version 6.2 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 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*.

- Changes to category-based URL filtering in Forcepoint NGFW version 6.1 affect all existing users of category-based URL filtering. Legacy URL Situation elements can no longer be used in policies for Forcepoint NGFW version 6.1 or later. If rules in your policy contain legacy URL Situation elements, you must replace them with URL Category elements. See the *Forcepoint Next Generation Firewall Product Guide* for detailed instructions.
- Starting from Forcepoint NGFW version 6.2, the Anti-Spam feature is no longer supported. See Knowledge Base article [12394](#). If you require this feature, we recommend that you use the most recent Long-Term Support (LTS) version. See Knowledge Base article [10192](#). If you require a comprehensive Anti-Spam and Email Security solution, we recommend that you use [Forcepoint Email Security Cloud](#).
- The way that routes defined in the Management Client are handled by Quagga has changed. In Forcepoint NGFW version 6.0 and earlier, static routes that you defined in the Management Client were considered kernel routes in Quagga. When redistributing these to dynamic routing protocols, you could use the "redistribute kernel" command.  
Starting from Forcepoint NGFW version 6.1.0, static routes that you define in the Management Client are considered static routes in Quagga. This change affects, for example, redistributing routes that you define in the Management Client to the dynamic routing protocols. Configuring static routes using vtysh in Quagga is no longer supported. Use the Management Client to configure static routing.

## Known issues

For a list of known issues in this product release, see Knowledge Base article [12476](#).

## Known limitations

This release of the product includes these known limitations.

| Limitation                                       | Description  |
|--|--|
| Inspection in asymmetrically routed networks     | In asymmetrically routed networks, using the stream-modifying features (TLS Inspection, URL filtering, and file filtering) can make connections stall.   |
| Inline Interface disconnect mode in the IPS role | The <i>disconnect mode</i> for Inline Interfaces is not supported on IPS virtual appliances, IPS software installations, IPS appliance models other than IPS-6xxx, or modular appliance models that have bypass interface 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, Knowledge Base articles, downloads, cases, and contact information.

# 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*
- *Stonesoft VPN Client User Guide* for Windows or Mac
- *Stonesoft VPN Client Product Guide*

