FORCEPOINT

Next Generation Firewall

Release Notes

6.2.3

Revision B

Contents

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
1101	FW, IPS, L2FW	Both images are supported
1105	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

Appliance model	Roles	Images
1402	FW, IPS, L2FW	Both images are supported
2101	FW, IPS, L2FW	Both images are supported
2105	FW, IPS, L2FW	Both images are supported
3201	FW, IPS, L2FW	Both images are supported
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
6205	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 6.2.3 build version is 18067.

Product binary checksums

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

- sg_engine_6.2.3.18067_x86-64.iso

```
SHA1SUM:
c632c748670401075ae32991ed1f2d271f1de728

SHA256SUM:
11bcde1b6e04a201d0a0aef69bfd8ad974af5ab15b791fd5fba8859947299d05

SHA512SUM:
0c396f2f4e53b7aea36d6644edb31ed8
30372cd9fa52bf3d817e056b4514b188
d9ec5d48bacaea16aa5d2f7c0393a8a1
aef576add6cb6b3669f1acec4069dbb3
```

- sg_engine_6.2.3.18067_x86-64.zip

```
SHA1SUM:
3071be0994a552127ae887958c6ef9ed5bc512cc

SHA256SUM:
b2f5960a31148e25bab47afd5a3341e31318e801d8e77ad2fffff4fadd1e0727

SHA512SUM:
43b543468be0b633d563bd2df281d02c
5af1c4ae74b879431d84f56a5bdca10b
22b6daa893d0bda1c3296f9033897830
5d49f58121edecdf2bc2ec16c4adc04d
```

- sg_engine_6.2.3.18067_x86-64-small.iso

```
SHA1SUM:
9c1294dfa7f6455528a34e3695d206ef17d196df

SHA256SUM:
77e9d5b37fb786334a71fc91f831aaeb3e5612b2f4ec7f915b18356686fb41cb

SHA512SUM:
48da7f7e93fe53fa3b869ae6eced1bc9
3f50a6bac7ace6c7772d6896e2dd4d46
7936e8437375bc50d87d55826a66f487
aa36fe705e46900de57219a80602ed04
```

- sg_engine_6.2.3.18067_x86-64-small.zip

```
SHA1SUM:
01f159dd916aaedb013865bb3f9357e4a323ce26

SHA256SUM:
4e9d38a5ac1f5d24277fd35a49b56b648ab92abefbec21da3ee5d79ed4492570

SHA512SUM:
db975bcb04d57a59cc500fd50e0c31bb
91b9225457ae42d1ccaa4414398c4e56
6e50a2456425e42a38df7fb26e29c72f
43af7a06cca7ad54db72a37ed9dd6ff2
```

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	A file allowed through an NGFW Engine and later found 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. 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.

Enhancements in Forcepoint NGFW version 6.2.2

Enhancement	Description
Log rate and spooled log information available in engine status monitoring	In the engine status monitoring, you can now see the log rate and the times at which logs have been spooled on the engine.
Improved dynamic routing monitoring	Changes in the OSPF and BGP neighborhood trigger alerts that are visible in the Logs view of the Management Client. Information about route changes is also included in logs.
Improved inspection for flash files	The NGFW Engine now supports the inspection of flash files, allowing it to detect potential security threats in flash files.
Faster rule matching for dynamic elements	Rule matching for rules that contain DNS names, users, and user groups is now faster. This improvement is especially useful when the policy uses a large number of these elements.

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
On Virtual Firewalls, some static routes might be removed if you move networks and routing configurations from one interface to another, or if you create a new Aggregated Link interface.	FW	NGFW-1275
If dynamic routing is configured, the routing table might have duplicate entries for some routes after you upgrade the NGFW Engine to version 6.2.	FW	NGFW-6311
When the NGFW Engine processes specific types of traffic, the inspection process might restart.	FW, IPS, L2FW	NGFW-7578
When you refresh the policy on the Master NGFW Engine, but not on the Virtual Firewall, the authentication page for browser-based user authentication might not load completely, or user authentication might time out soon after a user authenticates if session handling is enabled on the User Authentication branch of the Engine Editor.	FW	NGFW-7875
If both an HTTP and an HTTPS port are defined, and "Always use HTTPS" is selected on the User Authentication branch of the Engine Editor, connections to the HTTP port are forwarded to the listening IP address for the HTTPS port even if the original connections use a DNS name. This issue can cause HTTPS connections to fail with a certificate error.	FW	NGFW-7982
DHCP requests sent by the NGFW Engine for mobile VPN clients might not be accepted by some DHCP servers.	FW	NGFW-8044
If a VPN client connection is not correctly terminated, such as when there are intermittent connectivity issues, and cluster load balancing allocates the new connection to another node in the cluster, more than one node in the cluster might have an active DHCP lease for the same IP address. This issue can prevent some connections.	FW	NGFW-8066
If DHCP relay is configured on multiple interfaces, including the interface through which the DHCP server is reached, the NGFW Engine might stop forwarding DHCP offers to clients even though the NGFW Engine receives DHCP offers.	FW	NGFW-8092
If the NGFW appliance has MOE10F4 (MOD-EM2-10G-SFP-4) or MO40F2 (MOD-40G-2) interface modules and the cluster state changes, such as when a node goes offline and then online, traffic might stop passing through the cluster.	FW	NGFW-8099
When a Master NGFW Engine node goes offline or online, or a Master NGFW Engine node restarts, the dynamic routing process might not start correctly on the Master NGFW Engine.	FW	NGFW-8122
When you delete a Virtual Firewall that has dynamic routing configured, the dynamic routing configuration is not deleted from the Master NGFW Engine. If you create a new Virtual Firewall that has uses same Virtual Resource, the new Virtual Firewall might start with the dynamic routing configuration from the deleted Virtual Firewall.	FW	NGFW-8163

Description	Role	Issue number
When you move a Virtual NGFW Engine to a different Master NGFW Engine node, IPv6 routes might not be propagated from the BGP configuration to the routing table for the Virtual NGFW Engine. Routes might be visible when you use VTYSH on the command line, but they do not appear in the Virtual NGFW Engine properties in the Management Client.	FW	NGFW-8192
When you remove a Virtual Firewall that has a route-based VPN tunnel of the GRE tunnel type, interface tests fail and only one Master NGFW Engine node stays online.	FW	NGFW-8228
The dynamic routing suite has been updated to address CVE-2017-16227.	FW	NGFW-8270
When the NGFW Engine requests a virtual IP address for a VPN client from a DHCP server, user and user group information might not be included in the request.	FW	NGFW-8340

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 *disconnect mode* 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*