FORCEPOINT

Next Generation Firewall

Release Notes

6.2.4

Revision A

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 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 6.2.4 build version is 18103.

Product binary checksums

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

- sg_engine_6.2.4.18103_x86-64.iso

```
SHA1SUM:
61136d8d2c394041a701ad681fc9475e7ac51a85

SHA256SUM:
1a092c2c0cb2647ce974cfeba92c24a37976705e09d7bcecbc7e898e1b0c458b

SHA512SUM:
fc564cf4de101432299ec41135be0d4e
059be17bc039fe6b3000fd3dd09d01d1
f5379e6c12bda3b34f628837a7ed806b
9880fa2f99f51caa7140ed9043468f04
```

- sg_engine_6.2.4.18103_x86-64.zip

```
SHA1SUM:
1683535405c8b1ea0ce41cafddd632df844922fa

SHA256SUM:
9b7ecbb82b69814cbf47f58525f5ff7848b3ab35f80ab4283417a4bbf2fdc799

SHA512SUM:
e6e74cd567e8756c687527cf4c9e5351
b8a06210bc8a851ef5773466163b1408
8f1912fb56ead37ff47aac1d4e242fc7
01cc9bbd51402a8cda04d8e3d3ac100f
```

- sg_engine_6.2.4.18103_x86-64-small.iso

  ```
  SHA1SUM:
  7e92869bf81a5ba6b3383c60afec7fc3a681244e

  SHA256SUM:
  184c121590548dea1f57d3c5d01e4c6bf3401994fec22e96d09615d064fdf948

  SHA512SUM:
  1da3b024f791b8224236ae8a66eb4eb0
  b4671aa897e6b376414b45fc0632302e
  2ad5af67d3773758ae32a6480f14caa4
  4c57c86c32de52de35773999614eb906
  ```

- sg_engine_6.2.4.18103_x86-64-small.zip

  ```
  SHA1SUM:
  4c92edc4fadce3c794356d823b4e4608263427c9

  SHA256SUM:
  b5d25a5c6b82e5b2c8c39080976f15cacead6f38725ee9cb2c6a5a83b4123418

  SHA512SUM:
  cf0fed1cd7a1464123d71cf61712a0f2
  d317433066f462ad8401c8b9adf7f7c4
  cd4467728916507c18bdbbbcee677f6d
  c8ccc16cd701888c83aa7244a0f5eef3
  ```

Compatibility

Forcepoint NGFW 6.2 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.2 or higher
- Dynamic Update 864 or higher
- Stonesoft® VPN Client for Windows 6.0.0 or higher
- Stonesoft® VPN Client for Mac OS X 2.0.0 or higher
- Stonesoft® VPN Client for Android 2.0.0 or higher
- Server Pool Monitoring Agent 4.0.0 or higher
- 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.

Enhancements in Forcepoint NGFW version 6.2.4

Enhancement	Description
IGMP-based multicast forwarding enhancement	When an NGFW Engine is used as an IGMP proxy for multicast forwarding, the number of supported multicast groups has increased.

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.

Description	Role	Issue number
If the NGFW Engine uses IGMP-based multicast forwarding (IGMP proxying), rebooting the NGFW Engine, or starting the sg-reconfigure script might take a long time.	FW	NGFW-6378
If an NGFW Engine is selected in the Home view of the Management Client, the memory consumption of the selected node might start to increase while the Home view remains open. The memory is released when you close the Management Client.	FW, IPS, L2FW	NGFW-7303
When you create a Virtual NGFW Engine for a Master NGFW Engine that has an aggregated interface that has VLANs allocated to the Master NGFW Engine, when the policy with the Virtual NGFW Engine configuration is installed, the Link Status engine test reports a failure.	FW	NGFW-8016
Two-factor authentication using the SSL VPN Portal does not work.	FW	NGFW-8375
When you change the duplex settings using sg-reconfigure on the NGFW Engine command line, the change is not applied. The NGFW Engine uses the "auto" duplex setting.	FW, IPS, L2FW	NGFW-8527
When an HTTP Protocol Agent has URL logging enabled, but the Access rule does not have deep inspection enabled, the URL is not logged.	FW, IPS, L2FW	NGFW-8537
When end users access an SSL VPN Portal Service using the direct URL of the service instead of logging on to the SSL VPN Portal, the users might not be redirected to the service after they authenticate.	FW	NGFW-8543
Refreshing the policy on a Virtual NGFW Engine that has active VPN connections might cause the Master NGFW Engine and its hosted Virtual NGFW Engines to stop processing traffic. You must restart the Master NGFW Engine to start processing traffic again.	FW	NGFW-8680
You cannot use the NGFW Initial Configuration Wizard (sg-reconfigure) in a web browser with 2100 series NGFW appliances.	FW, IPS, L2FW	NGFW-8683
When the NGFW Engine uses a legacy firewall-only license that does not include full inspection, inspection of the protocols that are allowed by the license might not work. Legacy firewall-only licenses allow the inspection of the following protocols: HTTP, HTTPS, DNS, SIP, IMAP, POP3, and SMTP.	FW	NGFW-8717
TLS decryption might not work for some connections. As a result, the connections fail. If category-based URL filtering is also applied to the decrypted connections, those connections fail.	FW, IPS, L2FW	NGFW-8769

Description	Role	Issue number
IPsec tunnels through a standby endpoint might be negotiated unnecessarily.	FW	NGFW-8774
In a route-based VPN tunnel which is of the type GRE, IP-IP, or SIT, traffic might stop being processed after the policy is refreshed.	FW	NGFW-8786
If an external IGMP proxy is configured to use IGMP version 3 and an NGFW Engine IGMP proxy is configured to use IGMP version 2, multicast traffic might not be forwarded successfully.	FW	NGFW-8875
If the Subject of a certificate request does not have a space after the comma, the NGFW Engine is not able to create the certificate request.	FW	NGFW-8935
If a policy that removes an interface or a VLAN interface is refreshed, the refresh might fail. The NGFW Engine might need to be restarted.	FW	NGFW-9014
When the NGFW Engine inspects certain types of traffic, memory consumption might increase substantially, inspected connections might experience high latency, or inspected connections might be dropped.	FW, IPS, L2FW	NGFW-9110
If a policy is installed or refreshed on an NGFW Engine that has a lot of static routes, all the static routes configured in the Management Client might not be present in the Quagga dynamic routing configuration.	FW	NGFW-9162
In rare cases, when a clustered NGFW Engine processes FTP connections, one node in the cluster might stop processing traffic.	FW, IPS	NGFW-9333
In rare cases, state synchronization might not work correctly with dynamic routing, or the policy upload might not finish successfully.	FW	NGFW-9439
On clustered NGFW Engines, if the node that is handling an inspected connection changes due to a failover in the cluster, the connection might become unresponsive.	FW	NGFW-9451
If the engine's routing table has a large number of entries, it might take a long time for the routing entries to appear in the Routing Monitoring view in the Management Client.	FW	NGFW-9500
Revision 0 of NGFW appliance models 2101 or 2105 might generate false high vbat alerts.	FW, IPS, L2FW	NGFW-9573
NGFW appliance models 1401 or 1402 might generate false alerts about the LAN NIC temperature.	FW, IPS, L2FW	NGFW-9629
If dynamic routing diagnostics are left enabled for a long time, the /spool partition on the NGFW Engine might become full.	FW	NGFW-9654
When an NGFW Engine or Virtual NGFW Engine on a Master NGFW Engine uses dynamic routing, connections to dynamically routed networks might be interrupted after a failover.	FW	NGFW-9787
When the "Enable Session Handling" option is enabled, the time-out for browser-based user authentication might be too strict when the client is slow to respond. Authentication might remove the user too aggressively, and rules that require authentication do not match until the user re-authenticates.	FW	NGFW-9904
The HTTP XFF Client column in the Logs view might be empty even when the connection that triggers the log entry contains this information.	FW, IPS, L2FW	NGFW-10246

Description	Role	Issue number
The dynamic routing suite for the NGFW Engine has been updated to address the following vulnerabilities: CVE-2018-5378, CVE-2018-5379, CVE-2018-5380, and CVE-2018-5381.	FW	NGFW-10257
When the NGFW Engine processes certain types of MSRPC traffic, the NGFW Engine might write excessively to the console, which can degrade the performance of the engine. As a result, traffic handling might be interrupted, and the node might go offline.	FW, IPS, L2FW	NGFW-10300

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.

Note: If you install the SMC on Windows 10 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 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 higher. If you have an lower 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 higher. 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 lower, 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*