FORCEPOINT

Next Generation Firewall

Release Notes

6.3.0

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 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 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.

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

Appliance model	Roles
FW-315	FW
320X (MIL-320)	FW
IPS-1205	IPS, L2FW
FWL321	FW
NGF321	FW, IPS, L2FW
FWL325	FW
NGF325	FW, IPS, L2FW
110	FW
115	FW
1035	FW, IPS, L2FW
1065	FW, IPS, L2FW
1101	FW, IPS, L2FW
1105	FW, IPS, L2FW
1301	FW, IPS, L2FW
1302	FW, IPS, L2FW
1401	FW, IPS, L2FW
1402	FW, IPS, L2FW
2101	FW, IPS, L2FW
2105	FW, IPS, L2FW
3201	FW, IPS, L2FW
3202	FW, IPS, L2FW
3205	FW, IPS, L2FW

Appliance model	Roles
3206	FW, IPS, L2FW
3207	FW, IPS, L2FW
3301	FW, IPS, L2FW
3305	FW, IPS, L2FW
5201	FW, IPS, L2FW
5205	FW, IPS, L2FW
5206	FW, IPS, L2FW
6205	FW, IPS, L2FW

Sidewinder S-series appliances

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

Appliance model	Roles
S-1104	FW
S-2008	FW
S-3008	FW
S-4016	FW
S-5032	FW
S-6032	FW

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.

- 4 GB RAM minimum
- 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)
  - Microsoft Hyper-V on Windows Server 2012 or Windows Server 2016 (Firewall/VPN role only)
    An Intel 64-bit processor is required.
- 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 6.3.0 build version is 19032.

Product binary checksums

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

- sg_engine_6.3.0.19032_x86-64-small.iso

```
SHA1SUM:
977560a68cb8cdcc84f442a87ecae1239efe965b

SHA256SUM:
cdbfd728c950c9e7ed8e48b825bf6c32edeecef10b79324ff9cbd699f89fe642

SHA512SUM:
c7e70ccf7fbba572373f6994f70da8c5
40321d5eca96694e9edc439c80211338
56e600bac73f9ae963403f9ab46f3ce7
c3e856bf5ae1f8022ec820add3ce3829
```

- sg_engine_6.3.0.19032_x86-64-small.zip

```
SHA1SUM:
92a490c7e5763219bf977c223cd81215fb19b325

SHA256SUM:
a782570eb6f909db126f5b8dd2226be10b253c95fe2ac8818a63e611d507c986

SHA512SUM:
90376f611b3ff1bc320956ecd696d8f1
ede23d90fc49c8b5cacaa4f3064e6999
75743675f8141434abc2294cf2eba14a
d4499e28c7f1010a35c850c8d6a11a23
```

Compatibility

Forcepoint NGFW 6.3 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.3 or later
- Dynamic Update 988 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

- Forcepoint Endpoint Context Agent (ECA) 1.0.0
- Forcepoint User ID Service 1.0
- McAfee® Logon Collector 2.2 and 3.0
- McAfee® Advanced Threat Defense 4.0

Note: Forcepoint NGFW 6.3 is the last major version that supports McAfee Logon Collector and McAfee Advanced Threat Defense.

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*.

Support for Forcepoint Endpoint Context Agent

Support for Forcepoint Endpoint Context Agent (ECA) allows you to use endpoint information in the Forcepoint NGFW policy to control access, identify users, and log their actions. ECA is a Windows client application that provides endpoint information to the NGFW Engine. ECA is a replacement for McAfee Endpoint Intelligence Agent (McAfee EIA).

CAUTION: If McAfee Endpoint Intelligence Agent (McAfee EIA) is configured on the NGFW Engine when you upgrade to version 6.3 or later, the NGFW Engine node is returned to the initial configuration state and stops processing traffic. You must remove the McAfee Endpoint Intelligence Agent (McAfee EIA) configuration and refresh the policy before you upgrade to version 6.3 or later. For more information, see Knowledge Base article 14093.

Multi-Layer Deployment for NGFW Engines in the Firewall/VPN role

Multi-layer deployment is now supported for NGFW Engines in the Firewall/VPN role. In multi-layer deployment, NGFW Engines in the Firewall/VPN role have both layer 2 physical interfaces and layer 3 physical interfaces. The same NGFW Engine can now provide the features of the Firewall/VPN role, as well as the inspection features of the IPS and Layer 2 Firewall roles.

Route-based VPN improvements

The user interface for configuring a route-based VPN has been improved. Instead of configuring a single Route-Based VPN element, you can create individual Route-Based VPN Tunnel elements. The route-based VPN tunnels can be used in Administrative Domains other than the Shared Domain.

Improvements in Forcepoint Advanced Malware Detection

In addition to the cloud sandbox, Forcepoint Advanced Malware Detection now also supports on-premises local sandboxes. Other improvements include the following:

- The NGFW Engine can now delay file transfers until the results of the sandbox scan are received.
- The NGFW Engine now separately requests a file reputation for each file in .zip archives.
- The reporting tools in the external portal have been improved, and it is easier to access reports in the external portal from the Management Client.

NGFW on Azure and Hyper-V

You can now deploy NGFW Engines in the Microsoft Azure cloud to provide VPN connectivity, access control, and inspection for services in the Microsoft Azure cloud. The Microsoft Hyper-V virtualization platform on Windows 2012 and 2016 servers is now also supported for NGFW deployment on a virtualization platform in a private cloud. Only NGFW Engines in the Firewall/VPN role are supported in the Microsoft Azure cloud and on the Microsoft Hyper-V virtualization platform.

Support for Forcepoint User ID Service

Forcepoint User ID Service collects information about users, groups, and IP addresses from Windows Active Directory (AD) servers and AD domains. You can use the information from the Forcepoint User ID Service in the Forcepoint NGFW policy to identify users and control access.

Support for HTTPS in Sidewinder HTTP Proxy

The Sidewinder HTTP Proxy can now provide decryption, inspection, protocol validation, certificate validation, and certificate revocation checking for the HTTPS protocol.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 6.3.0

Enhancement	Description
Rate limit per Virtual NGFW Engine for traffic from the Master NGFW Engine	You can now set a rate limit per Virtual NGFW Engine for traffic from the Master NGFW Engine to the Virtual NGFW Engine. When the limit is set, a single Virtual NGFW Engine that is under very heavy load cannot disrupt the operation of the other Virtual NGFW Engines that are hosted by the Master NGFW Engine.

Enhancement	Description
Dedicated control plane operation	You can now dedicate a specified number of CPUs to control plane operations. Even under very heavy loads, you can continue to manage NGFW Engines and refresh policies, and the status of the NGFW Engines remains green in the Home view.
Changes related to certificates	The NGFW Engine can now validate certificates and check the certificate revocation status for features that have certificate validation and certificate revocation checks enabled, such as features that use a TLS Profile in the configuration. Except for VPN certificates, most elements related to certificates are now found in the **Administration** > **Certificates** branch of the **Configuration** view. There is no longer a separate Pending Certificate Request element. Certificate requests are now created as TLS Credentials elements. The state of the TLS Credentials element indicates whether is it a signed certificate or a certificate request.
Limit for half-open TCP connections	As part of the SYN flood protection feature, you can now set a limit for the number of half-open TCP connections. When the limit is reached, SYN flood protection is enabled.
Improvements to SSM architecture	Improvements to SSM integration remove some previous limitations on inspection when Sidewinder Proxies are used. These former limitations include matching traffic based on Network Applications, file filtering, and URL filtering. New Combined Protocol elements allow you to apply a standard Protocol element and a Sidewinder Proxy Protocol element to the same traffic.
New commands for managing NGFW Engines and NGFW appliances	It is now possible to power off an NGFW Engine remotely through the Management Client. In addition, you can now also reset an NGFW appliance to factory settings through the Management Client. To increase security, you can set how many times you want the stored data on the file system of the NGFW appliance to be overwritten.
Task for validating policies	There is a new task for validating policies. The Validate Policy task allows you to validate the policy installed on NGFW Engines or Master NGFW Engines or the Alert Policy installed in an administrative Domain. You can run the Validate Policy task either manually or according to a schedule.
SYN rate limits support IPv6 connections	SYN rate limits now also support IPv6 connections.
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
The tcpdump utility that is included in the NGFW Engine software has been updated to version 4.9.2 to address multiple potential security and denial of service issues.	FW, IPS, L2FW	NGFW-2998
After the certificate for an engine node has been renewed, the engine might continue to use a backup of the previous certificate instead of the new certificate. This issue can happen after automatic certificate authority (CA) renewal, when the type of CA changes, or after automatic node certificate renewal.	FW, IPS, L2FW	NGFW-3178
When you use the cloud sandbox for Forcepoint Advanced Malware Detection, memory consumption can increase significantly.	FW, IPS, L2FW	NGFW-4468
When you use McAfee GTI, memory consumption might increase significantly and cause the NGFW Engine to become unstable.	FW, IPS, L2FW	NGFW-4554
If deep inspection records the matching traffic, some CPUs can be fully utilized, which causes traffic to be processed slowly for some connections.	FW, IPS, L2FW	NGFW-4637
When the SSM HTTP Proxy processes certain types of HTTP traffic, the proxy process might restart.	FW	NGFW-4942
If you configure protocol-independent multicast (PIM) routing using the Management Client, then change the PIM configuration on the command line using VTYSH, the PIM configuration files might be overwritten.	FW	NGFW-5110
If you disable a node in a cluster, but do not remove it from the network, when you refresh the policy in the other nodes in the cluster, there can be issues with state synchronization until the NGFW Engines are restarted. You should only disable a node when a cluster member has failed and hardware needs to be replaced. A cluster member that is present in the network must not be disabled.	FW, IPS, L2FW	NGFW-5229
When VPN tunnels are negotiated with a large number of different endpoints, the memory consumption in the NGFW Engine might increase substantially.	FW	NGFW-5251
If the "Log URL Categories" option is set to "Enforced" in the logging options, TLS connections might not be decrypted even if TLS decryption is enabled for the NGFW Engine.	FW, IPS, L2FW	NGFW-5282
If the NGFW Engine is processing both IPv4 and IPv6 traffic, some related connections might not get through.	FW, IPS, L2FW	NGFW-5435
If the rule that allows FTP connections matches Network Applications or logs information about application detection, but does not have deep inspection or file filtering enabled, related connections for FTP might not be allowed.	FW, IPS, L2FW	NGFW-5477
When file filtering blocks a file, and a user response is configured for the connection, some CPUs can be fully utilized, which causes traffic to be processed slowly for some connections.	FW, IPS, L2FW	NGFW-5705

Description	Role	Issue number
If a VPN configuration is large and refreshing the policy causes a large number of tunnels to be reconfigured, the refreshing of the policy can time out.	FW	NGFW-5708
The NGFW Engine might be unstable with newer CPU models due to incompatible features that have been enabled.	FW, IPS, L2FW	NGFW-5844
In rare cases, the inspection process or the NGFW Engine might restart when file filtering or deep inspection is applied to traffic.	FW, IPS, L2FW	NGFW-5861
When the engine inspects specific tunneled traffic, the engine might restart in the following cases: • A rule in the Inspection Policy uses the "Terminate: Passive and Silent" action to log that termination could have occurred, but does not stop the traffic. • The value of the "Action if Limit Exceeded" option for "Limit for Rematching Tunneled Traffic" is "Allow".	IPS, L2FW	NGFW-5865
When the Tunnel Type is "VPN" for a tunnel in the route-based VPN and you use OSPF dynamic routing with the tunnel, routing information received from a neighbor might not be accepted.	FW	NGFW-5899
When a Virtual NGFW Engine is moved to a different Master NGFW Engine node, IPv6 routes might not be propagated from BGP to the routing table for the Virtual NGFW Engine. Routes might be visible when you use VTYSH, but they do not appear in the Virtual NGFW Engine.	FW	NGFW-5901
When you use a Virtual Firewall as a VPN endpoint and you use certificates for authentication, VPN negotiation might fail if there are too many simultaneous VPN tunnel negotiations.	FW	NGFW-5904
When you use loose connection tracking mode and connections are closed in a specific way, the connections are not removed from the engine's connection table until the idle timeout limit is reached. The existing connection prevents new connections from being established with the same source and destination IP addresses and ports until the existing connection is removed from the connection table.	FW, IPS, L2FW	NGFW-6046
When dynamic routing fails over, synchronized forwarding information base (FIB) routes might not be removed correctly.	FW	NGFW-6193
If you do not use an HTTP proxy to connect to the ThreatSeeker Intelligence Cloud server, URL filtering status is not shown on the status card for the NGFW Engine.	FW, IPS, L2FW	NGFW-6210
When you remove an automatic blacklist entry that was created by an engine from the Blacklist view, the command fails. The following message is shown: "Command failed (113)".	FW, IPS, L2FW	NGFW-6265
If Access rules use the FTP Protocol Agent and deep inspection is not enabled, the NGFW Engine might restart when you install the policy after adding or removing an interface.	FW	NGFW-6500
When you use a fully qualified domain name (FQDN) as the contact address for a VPN endpoint, and the DNS resolution changes, VPN connections stop working.	FW	NGFW-6602

Description	Role	Issue number
If a Virtual Firewall is used as a VPN gateway, and the Virtual Firewall is moved to a different Master NGFW Engine node, VPN traffic might be disrupted until the VPN tunnels are renegotiated.	FW	NGFW-6607
Certain types of TCP keep-alive packets might be dropped if deep inspection is enabled.	FW, IPS, L2FW	NGFW-6858
Logs of the type Connection_Allowed do not show the destination interface, destination VLAN, or destination zone if the connection that generated the log entry was inspected.	FW, IPS, L2FW	NGFW-7142
If SNMP is configured, it does not work with interfaces that have PPP enabled.	FW	NGFW-7223
When a concurrent connection limit is configured and set to Refuse in the action options of an Access rule, the NGFW Engine might become unresponsive until you restart the NGFW Engine.	FW, IPS, L2FW	NGFW-7311
If IPv6 addresses have been configured for a Virtual NGFW Engine, the Master NGFW Engine might restart when the policy is installed or refreshed.	FW	NGFW-7340

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.

CAUTION: If McAfee Endpoint Intelligence Agent (McAfee EIA) is configured on the NGFW Engine when you upgrade to version 6.3 or later, the NGFW Engine node is returned to the initial configuration state and stops processing traffic. You must remove the McAfee Endpoint Intelligence Agent (McAfee EIA) configuration and refresh the policy before you upgrade to version 6.3 or later. For more information, see Knowledge Base article 14093.

Note: 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.

Note: 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.

- Upgrading to version 6.3 is only supported from version 5.10 or later. If you have an earlier version, first upgrade to version 5.10.
- Forcepoint NGFW version 6.3 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*.
- If you have customized the sshd_config file in the /data/config/ssh directory, you might need to manually update the configuration file after upgrading the engine to Forcepoint NGFW version 6.3. See Knowledge Base article 10461.

Known issues

For a list of known issues in this product release, see Knowledge Base article 14124.

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.

Limitation	Description
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*