FORCEPOINT

Next Generation Firewall

Release Notes

6.3.3

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 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 6.0 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 6.3.3 build version is 19153.

Product binary checksums

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

- sg_engine_6.3.3.19153_x86-64-small.iso

```
SHA1SUM:
dc09fa11fa9c102fe44c096c4154ff6ee11f1221

SHA256SUM:
5a7e9c366a754b1ce8af9601bcbf861c50dd79a09159df5bc0ca2c5b903c3c41

SHA512SUM:
71f181e2f47106d937783621ac31ff8b
6f51f5038e7200f1a39fcbfc0a73529e
39a764ea43bd3f52cb1cf495068b7e05
b7bf3f690d44a0673a61413a1d94d276
```

- sg_engine_6.3.3.19153_x86-64-small.zip

```
SHA1SUM:
32c9e7ee5aab3fe2c111745625b7ab4149fb672f

SHA256SUM:
5b970d9470fb84aff2a9a2fe20fba6acde286faf01ab9626f5c0283a11f5b1db

SHA512SUM:
43dbd76a5a33f51165dca49dec57c1e6
2339dbf11074e92239d1c112aa1c9421
0e3a316eeda2089a05d5ece8996de72f
822c5ecb1db125230b6a735922ceabe6
```

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) 1.1.0
- Forcepoint User ID Service 1.1.0
- 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 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.

Enhancements in Forcepoint NGFW version 6.3.2

Enhancement	Description
Dynamic routing throughput improved	The throughput of dynamically routed packets has improved.
SNI in TLS communications for the SSL VPN Portal	The SSL VPN Portal now uses the server name indication (SNI) in TLS communications between the NGFW Engine and web resources.
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.

Enhancements in Forcepoint NGFW version 6.3.3

Enhancement	Description
QoS throughput alerts added	An alert is now triggered when the QoS throughput limit defined for a Virtual Security Engine is exceeded.
Additional cipher support added	Client and server protection features now support additional ciphers.

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
When you add or remove an Aggregated Link interface, traffic that uses the Aggregated Link interfaces might be interrupted.	FW	NGFW-5031
When a rate limit is configured on a Virtual NGFW Engine, traffic might be dropped even when the traffic rate is below the configured limit.	FW, IPS, L2FW	NGFW-7795
If a node in a cluster is rebooted, Access rules that reference User Groups provided by the Forcepoint Endpoint Context Agent (ECA) might not match traffic on the node that was rebooted for up to 30 minutes.	FW, IPS, L2FW	NGFW-8249
In rare cases, when a clustered NGFW Engine processes FTP connections, one node in the cluster might stop processing traffic.	FW, IPS	NGFW-9333
Connections that are inspected by the NGFW Engine might not be closed properly in one of the communicating endpoints if another endpoint uses an RST (reset) to initiate closing the connection.	FW, IPS, L2FW	NGFW-9339
This maintenance release includes support for optional hardening against CPU vulnerabilities that have been branded as Meltdown and Spectre (CVE-2017-5715, CVE-2017-5753, and CVE-2017-5754). Hardening is not enabled by default. For more information, see https://support.forcepoint.com/KBArticle?id=000014989.	FW, IPS, L2FW	NGFW-9362

Description	Role	Issue number
If inspection is not enabled by a policy and an NGFW Engine in the Firewall/VPN role is configured with an inline IPS interface where the Failure Mode is Bypass, the inline interface can go into bypass mode, even though the NGFW Engine is online.	FW	NGFW-9443
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 routing table for an NGFW Engine 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
The Enforce TCP MSS option might not be applied to related connections when connections are inspected.	FW, IPS, L2FW	NGFW-9578
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
If a new dynamic update package has been activated, when the policy is refreshed on multiple Virtual NGFW Engines in a Master NGFW Engine cluster at the same time, the Master NGFW Engine nodes might restart.	FW, IPS, L2FW	NGFW-9678
Client or server protection might not work for connections which require using ECDH key exchange.	FW, IPS, L2FW	NGFW-9766
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
An issue with the drivers for a gigabit interface might cause the NGFW Engine to go offline. The related dmesg messages contain "Detected Tx Unit Hang".	FW, IPS, L2FW	NGFW-10181
Connections to Microsoft services that are subject to client or server protection and file filtering might not work.	FW, IPS, L2FW	NGFW-10194
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
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

Description	Role	Issue number
NetLink and policy-based routes that are configured in the NGFW Engine create static default route entries in the dynamic routing suite routing table, even though these routes match only part of the traffic.	FW	NGFW-10357
Two-factor authentication when authenticating using a Radius server might not work.	FW	NGFW-10471
Inspecting HTTPS connections can cause instability in the inspection process in certain circumstances.	FW, IPS, L2FW	NGFW-10530
NGFW Engines that have PPP interfaces might restart, and kerneldump files might be created.	FW	NGFW-10552
The DHCP software for the NGFW Engine has been updated to address the following vulnerability: CVE-2018-5732.	FW, IPS, L2FW	NGFW-10571
If the same AS number is prepended multiple times for a BGP Route Map in the SMC configuration, the AS number is prepended only once in the Route Map when checking it using vtysh.	FW	NGFW-10660
When a policy is installed or refreshed, dynamic routing processes might restart unnecessarily.	FW	NGFW-10661

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.

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.
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*