FORCEPOINT

Next Generation Firewall

Release Notes

5.10.11

Revision B

Contents

About this release

This document contains important information about this release of Forcepoint™ Next Generation Firewall (Forcepoint NGFW; formerly known as McAfee® Next Generation Firewall). We strongly recommend that you read the entire document.

NGFW version 5.10.1 has been evaluated against the Common Criteria Network Devices Protection Profile with Extended Package Stateful Traffic Filter Firewall. For more details, see https://www.niap-ccevs.org/Product/Compliant.cfm?pid=10669.

Note: We have started rebranding the NGFW product and the NGFW product documentation. We use Stonesoft as the product name in this document. However, the old product name is still used in the NGFW appliances and the product documentation set that we created for the NGFW 5.10.0 release.

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.

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 (F), 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
1035	FW, IPS, L2FW	Both images are supported
1065	FW, IPS, L2FW	Both images are supported
1301	FW, IPS, L2FW	Both images are supported
1302	FW, IPS, L2FW	Both images are supported
1401	FW, IPS, L2FW	Both images are supported
1402	FW, IPS, L2FW	Both images are supported
2101	FW, IPS, L2FW	Both images are supported
2105	FW, IPS, L2FW	Both images are supported

Appliance model	Roles	Images
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 CD 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 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 Security 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 5.5 and 6.0

    Note: Forcepoint Next Generation Firewall 5.10.11 does not support integration with Intel Security Controller and deployment on VMware NSX.
  - KVM (KVM is tested as shipped with Red Hat Enterprise Linux Server 7.0)
  - Oracle VM server 3.3 (tested with Oracle VM server 3.3.1)
- 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 Next Generation Firewall 5.10.11 build version is 14115.

Product binary checksums

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

- sg_engine_5.10.11.14115_x86-64.iso

```
SHA1SUM:
a5496eff67aaf36d92c0dfd2a7b52ab89cae2c0e

SHA256SUM:
2df46278f852df0b283a059a6d17dd4c22b58baf06a0a1eaab766bf0f693f5ff

SHA512SUM:
c9539a28f3c41c7cadbb423fb047bd8b
50f0a0c287673e5db96dd62b0f4971ba
3aa090d9176e1e787feed32fc757aa58
18c0ac236ca9d978b88d13b52e7fd90d
```

- sg_engine_5.10.11.14115_x86-64.zip

```
SHA1SUM:
bba5f36c69181e24ad33ac18c837b7ea46024bef

SHA256SUM:
6ce5fc4d22da154812b4d568ef99be2b15419303ba9f5835a10eaaa98b8ed7c8

SHA512SUM:
d94965434d0ac94fb5fce01fe05b59a1
a00755b96f5b419463a3409517978247
18f0aca040e663af4d11f505027727ec
bf1b7ecb968ac4756c26e96dc525ba71
```

- sg_engine_5.10.11.14115_x86-64-small.iso

```
SHA1SUM:
c2769067774a6c3f5ac66c8eebd1477f9b7c3ba0

SHA256SUM:
26cf22882ed5f2ddc7d099e4210b05bb1aa51aca4e5241b8f34694edf98b9eb3

SHA512SUM:
ef971cd2b1cf4df1c4248b7c278d24c8
41198c61e305bd99a0fec7753dbb9510
4758706da7c9f80075147b35885b7303
83b8e97156a8c72c9bf57a6f4de7d435
```

- sg_engine_5.10.11.14115_x86-64-small.zip

```
SHA1SUM:
f8957ec43719e6d778ad332cd2caa9a18b67a1a4

SHA256SUM:
ea76345bfdd6725bb6dbe42c757bdacf6a5f337954f375f7d1f62b88ae5c645b

SHA512SUM:
7918d6826ad92a4b7a402d1f9efbb8e8
fe61aa3809d602db3febb93b4ba8d5a1
c3c6f7e0b56b172c85555f91dedd8e32
4e7516dec3481cd9763efeb37cbd0d65
```

Compatibility

Forcepoint NGFW 5.10.11 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) (formerly known as McAfee® Security Management Center) 5.10.0 or later
- Dynamic Update 810 or later
- Stonesoft IPsec VPN Client 5.3.0 or later
- Stonesoft® VPN Client (formerly known as McAfee® VPN Client for Windows) 5.9.0 or later
- Stonesoft® VPN Client for Mac OS X (formerly known as McAfee® VPN Client for Mac OS X) 1.0.0 or later
- Stonesoft® VPN Client for Android (formerly known as McAfee® VPN Client for Android) 1.0.1 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*.

Note: Forcepoint Next Generation Firewall 5.10.11 does not support integration with Intel Security Controller and deployment on VMware NSX.

Support for Threat Intelligence Exchange

Forcepoint NGFW can now query file reputations and receive reputation updates from the McAfee® Threat Intelligence Exchange (TIE) server. TIE makes it possible for administrators to tailor comprehensive local threat intelligence from global intelligence data sources, such as McAfee® Global Threat Intelligence™ (McAfee GTI), endpoints, gateways, and other security components. File reputation data is exchanged using the McAfee® Data Exchange Layer (DXL) broker network. File reputation updates ensure that Forcepoint NGFW engines always have the latest file reputations available for use in file filtering.

Single sign-on (SSO) to SSL VPN Portal

The SSL VPN Portal (reverse web proxy) can be configured to cache user credentials. The portal logs on to the back-end servers with the credentials as if they came from the web browser at the endpoint. You can group the servers that use the same credentials by SSO domain, to further reduce the need to re-enter the password.

New tunnel type for the route-based VPN

A new tunnel type for the route-based VPN allows the use of tunnel mode IPsec without an additional tunneling layer. The route-based VPN configuration dialog box has been improved.

Connectivity between Forcepoint NGFW and SMC using IPv6

Engines that only use IPv6 to connect to the Internet can now be managed by SMC over the Internet using IPv6-based management connections. Connectivity between SMC components still requires IPv4 addressing and connectivity.

Network Security for Industrial Control Systems (ICS)

ICS support has been enhanced with deep inspection support for DNP3 (TCP/UDP) and Open Platform Communications Unified Architecture (OPC UA).

Safe search support

Forcepoint NGFW can be configured to enforce safe search usage for Google, Bing, Yahoo, and DuckDuckGo web searches.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 5.10

Enhancement	Description
Advanced Threat Defense communication logging improvements	Improvements have been made to the communication protocol and logging features between McAfee® Advanced Threat Defense and Forcepoint NGFW. Forcepoint NGFW now logs the dynamic analysis results when available from Advanced Threat Defense. Forcepoint NGFW provides the file name, destination IP address, and URL details when sending the file to Advanced Threat Defense for analysis.
File filtering improvements	Improvements have been made to file type detection and filtering. We recommend that you update your file filtering policies with the new file type categories.
DHCP services	It is now possible to use DHCP server and DHCP relay services on different interfaces of the same Forcepoint NGFW engine.

Enhancements in Forcepoint NGFW version 5.10.3

Enhancement	Description
Dynamic routing enhancements	Dynamic routing features, such as graceful restart for OSPF and BGP, have been improved. The stability of dynamic routing has also been improved.

Enhancements in Forcepoint NGFW version 5.10.4

Enhancement	Description
Improved alerting for offline transitions	Alerting for offline transitions has been improved. Alerts are now created for unexpected offline transitions, such as heartbeat recovery, or nodes that have different policies.
Faster policy installation for Virtual Security Engines	Policy installation is now faster in environments that have many Virtual Security Engines.

Enhancements in Forcepoint NGFW version 5.10.8

Enhancement	Description
Engine monitoring enhancements	Engine monitoring has been improved. If the monitoring connection through a primary Control Interface fails, the backup Control Interface is used.

Enhancement	Description
Improved logging for File Filtering	Logging for File Filtering has been improved significantly. For example, all File Filtering Situations are now logged under File Filtering in the Facility column of the Logs view.
Inspection with a larger number of Virtual Security Engines	Inspection can now be used with a larger number of Virtual Security Engines that are hosted on a single Master Engine.

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
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
If the Quality of Service (QoS) mode "QoS Statistics Only" is configured for some interfaces while other interfaces use other QoS modes, the engine might stop processing traffic.	FW, IPS, L2FW	NGFW-4551
If deep inspection logs the record of the matching traffic, some CPUs can be fully utilized, which causes traffic to be processed slowly for some connections.	FW, IPS, L2FW	NGFW-4637
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 NGFW Engine is processing both IPv4 and IPv6 traffic, some related connections might not get through.	FW, IPS, L2FW	NGFW-5435
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

Description	Role	Issue number
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 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 you configure a route map for a BGP announced network using the Management Client, the route map is not added to the announced network in the dynamic routing configuration.	FW	NGFW-6128
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

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 **Security Engine 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 5.10.x is only supported from version 5.8.x or later. If you have an earlier version, first upgrade to the latest 5.8.x version.
- Forcepoint NGFW 5.10.x requires an updated license if upgrading from version 5.9.x or earlier. 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 CD and follow the instructions. For detailed instructions, see the *Forcepoint Next Generation Firewall Installation Guide*.

Take the following software architecture information into consideration.

- Forcepoint NGFW appliances support only the software architecture version with which they come installed. 32-bit versions (i386) can only be upgraded to another 32-bit version and 64-bit versions (x86-64) can only be upgraded to another 64-bit version.
- Clusters can only have online nodes that use the same software architecture version.
- State synchronization between 32-bit and 64-bit versions is not supported.
- Changing the architecture of third-party servers using software licenses requires the software to be fully re-installed from a CD.
- Forcepoint NGFW version 5.10 only supports 64-bit software architecture. Except for the FW-315 appliance, the last supported software version for 32-bit Firewall/VPN appliances is 5.8.
- To upgrade a cluster (consisting of FW-315 appliances or third-party hardware using software licenses) from a 32-bit to 64-bit version, see Knowledge Base article 9875.

Known issues

For a list of known issues in this product release, see Knowledge Base article 10138.

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.
SSL/TLS inspection in capture (IDS) mode	Due to SSL/TLS protocol security features, SSL/TLS decryption in capture (IDS) mode can only be applied in a server protection scenario when RSA key exchange negotiation is used between the client and the server.

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.

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.

- *Stonesoft Next Generation Firewall Product Guide*
- Stonesoft 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.
- *Stonesoft Next Generation Firewall Installation Guide*

Other available documents include:

- *Stonesoft Next Generation Firewall Hardware Guide* for your model
- *Stonesoft Next Generation Firewall Quick Start Guide*
- *Stonesoft SMC API Reference Guide*
- *Stonesoft VPN Client User Guide* for Windows or Mac
- *Stonesoft VPN Client Product Guide*