



FORCEPOINT

Next Generation Firewall

Release Notes

6.4.4

Revision A

Contents

- [About this release](#) on page 2
- [Lifecycle model](#) on page 2
- [System requirements](#) on page 3
- [Build version](#) on page 6
- [Compatibility](#) on page 7
- [New features](#) on page 7
- [Enhancements](#) on page 8
- [Resolved issues](#) on page 10
- [Installation instructions](#) on page 11
- [Known issues](#) on page 13
- [Find product documentation](#) on page 13

About this release

This document contains important information about this release of Forcepoint Next Generation Firewall (Forcepoint 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

To use this product, your system must 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
320X (MIL-320)	FW
FWL321	FW
NGF321	FW, IPS, L2FW
FWL325	FW
NGF325	FW, IPS, L2FW
110	FW
115	FW
330	FW, IPS, L2FW
331	FW, IPS, L2FW
335	FW, IPS, L2FW
1035	FW, IPS, L2FW
1065	FW, IPS, L2FW
1101	FW, IPS, L2FW
1105	FW, IPS, L2FW
1401	FW, IPS, L2FW
1402	FW, IPS, L2FW
2101	FW, IPS, L2FW
2105	FW, IPS, L2FW
3202	FW, IPS, L2FW
3206	FW, IPS, L2FW
3207	FW, IPS, L2FW
3301	FW, IPS, L2FW

Appliance model	Roles
3305	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
The following network interface card drivers are recommended:
 - VMware ESXi platform — `vmxnet3`.
 - KVM platform — `virtio_net`.

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.

Supported cloud environments

You can deploy Forcepoint NGFW in the Amazon Web Services (AWS) and Microsoft Azure cloud environments.

Amazon Web Services

Forcepoint NGFW instances can be launched from AWS using 1-Click Launch, and existing instances can be remotely upgraded to the latest Forcepoint NGFW version.

To see the currently available instance types, search for *Forcepoint NGFW* in the AWS Marketplace.

For more information about deploying in AWS, see the document *How to deploy Next Generation Firewall in the Amazon Web Services cloud* and Knowledge Base article [10156](#).

Microsoft Azure

Forcepoint NGFW instances can be launched from Azure using custom solution templates, and existing instances can be remotely upgraded to the latest Forcepoint NGFW version.

To see the currently available custom solution templates, search for *Forcepoint NGFW* in the Azure Marketplace.

For more information about deploying in Azure, see the document *How to deploy Next Generation Firewall in the Azure cloud* and Knowledge Base article [14485](#).

Build version

Forcepoint NGFW 6.4.4 build version is 20203.

Product binary checksums

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

- `sg_engine_6.4.4.20203_x86-64-small.iso`

```
SHA1SUM:
08041d94ae3128e891b8258ba5e468d8298bb4d0

SHA256SUM:
b335f7aa29fad1803d6fe01dfc903d0cdf8a8a58ae9343900e1a60e3c193b57b

SHA512SUM:
4b2ecaff3a2de2896ce88fc08d6c0448
61156ffb6535c470f4ea5b423c2f662c
db454c30b5b15e1b640e1866b9a7c500
24d201b630549a4fc5da326a8a559b20
```

- `sg_engine_6.4.4.20203_x86-64-small.zip`

```
SHA1SUM:  
d291ad6402ec513c88e926b9d374c82acf9d6728  
  
SHA256SUM:  
aa3d5b855523217aec5c14329f327397f5b9f2e6fc5e509ca179af19ed5e1c15  
  
SHA512SUM:  
fb04a821007693028f5c5be5e04f1525  
8abb9b90df2d42b9af3e0c63f335b9f  
efe796c9d3c251546ac49fdc422199  
c5133b6a85ff4ed6731d5c9c6d2764dd
```

Compatibility

Forcepoint NGFW 6.4 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.4 or higher
- Dynamic Update 1041 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
- Forcepoint Endpoint Context Agent (ECA) 1.1.0 or higher
- Forcepoint User ID Service 1.1.0 or higher
- McAfee® Logon Collector 2.2 and 3.0

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*.

Redirection of HTTP and HTTPS traffic to a proxy

The NGFW Engine can now transparently redirect HTTP and HTTPS traffic to a proxy. The proxy can be on-premises or a cloud-based service, such as the Forcepoint Web Security Cloud service. The traffic does not have to be redirected through a policy-based VPN.

Improved integration of external NTP servers

You can now use external NTP servers to provide time synchronization for both the SMC Appliance and NGFW Engines. External NTP servers were previously supported only for the SMC Appliance. You can use the same NTP servers for the SMC Appliance and the NGFW Engines.

SNMP Agent enhancements

You can now use SNMP Agents when you configure SNMP for the SMC Appliance. SNMP Agents were already supported for NGFW Engines in previous versions.

You can now specify the SNMP engine ID for each NGFW Engine and for the SMC Appliance. The SNMP engine ID is a unique identifier that the SNMP Agent uses to for the NGFW Engine or the SMC Appliance.

SNMP Agents now support IPv6 addresses.




Note: If you configured SNMP for the SMC Appliance before upgrading to version 6.4, you must configure SNMP again after upgrading to version 6.4.0 or higher.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 6.4.0

Enhancement	Description
Improved integration of external LDAP servers and Active Directory servers	<p>The integration of external LDAP servers and Active Directory servers with Forcepoint NGFW has been improved.</p> <ul style="list-style-type: none"> Support for the LDAPS and Start TLS protocols for securing the LDAP connection has been improved. When LDAPS or Start TLS is enabled for an LDAP Server or Active Directory Server, you can now select a TLS Profile and TLS Server Identity for the LDAP Server. A new Authentication Method element for LDAP Authentication has been added. When LDAP Authentication is configured for a user, the user's password is checked against the user's credentials in the LDAP server that is used for user storage. LDAP Authentication can be used with the following existing features: IPsec and SSL tunnels in mobile VPNs, the SSL VPN Portal, and browser-based user authentication.
Improvements in browser-based user authentication	<p>Browser-based user authentication now supports certificate-based authentication. Users can authenticate using a certificate file, or a certificate stored on a smart card, such as a Common Access Card (CAC).</p>
Other authentication enhancements	<p>The Require Authorization and Timeout for Client IP Authorization options have been removed from Authentication options for Access rules. Authorization is automatically required when you add User and Authentication Method elements to the Authentication cell. The Authentication Time-Out option in the Add-Ons > User Authentication branch of the Engine Editor replaces the Timeout for Client IP Authorization option.</p>

Enhancement	Description
Improvements in application detection	<p>Because Access rules for application detection match traffic based on the payload of connections, the same connection can potentially match more than one rule based on the first SYN packet of the connection. Connection handling such as the use of VPNs, NAT, SSM Proxies, and TCP MSS enforcement is applied according to the initial match. When the final match is different from the initial match in a way that changes connection handling, the connection is dropped. In these cases, a log message that indicates a conflict between rules is generated.</p> <div>  <p>Note: Due to changes in application detection, policies that use Network Applications, URL Categories, or URL Lists in the Access rules might work differently after upgrading to NGFW 6.4. Some traffic that was previously allowed might be discarded. After upgrading to NGFW 6.4 or higher, verify that your policies work as expected. For more information, see Knowledge Base article 15411.</p> </div>
New Network Application elements of the Cloud Services type	New Network Application elements of the Cloud Services type have been added to the SMC from the Forcepoint cloud access security broker (CASB) service catalog. Including the previous Network Application elements of the Web Applications and Protocols types, there are now over 7000 Network Applications available.
Duplicate IPv6 address detection for Layer 3 Physical Interfaces	An option for detecting duplicate IPv6 addresses has been added to the Layer 3 Physical Interface properties for NGFW Engines.
Bootloader password for NGFW Engines	During the initial configuration, you can now specify a bootloader password for the NGFW Engine. To edit the options that appear in the bootloader, you must enter the bootloader password.
Layer 2 Physical Interfaces on Virtual Firewalls and Master Engines that host Virtual Firewalls	You can now configure Layer 2 Physical Interfaces on Virtual Firewalls and Master Engines that host Virtual Firewalls.
Easier deployment of NGFW Engines in Microsoft Azure	You can now deploy NGFW Engines from the Microsoft Azure cloud environment without first creating the NGFW Engine element in the Management Client. You deploy the NGFW Engines from the cloud environment, and you can monitor the NGFW Engines in the Management Client.
Auto-scaling in Microsoft Azure	Support for auto-scaling for NGFW Engines that are deployed in Azure has been added. When the scaling feature is used, additional NGFW Engine instances are automatically created and removed, depending on traffic load. You can monitor the NGFW Engine instances in the Management Client.
Cloud Sandbox analysis information in the external portal	You can now view analysis information in the external portal for the cloud sandbox. You must define a user name for the cloud service in the Management Client to be able to view the analysis information in the external portal.
Auto-discovery for ECA clients	The NGFW Engine can now advertise its contact address to ECA clients. If the contact address of the NGFW Engine changes, or a new NGFW Engine is added to the network, the ECA clients are still able to connect to the NGFW Engine.
Monitoring of Forcepoint User ID Service	You can now enable monitoring for the Forcepoint User ID Service. You can also configure that the Forcepoint User ID Service sends log data to the SMC.
License reporting tool	There is a new tool for MSSP customers that exports all data related to licenses and NGFW Engines to a CSV file.

Enhancements in Forcepoint NGFW version 6.4.1

Enhancement	Description
QoS throughput alerts added	An alert is now triggered when the QoS throughput limit defined for a Virtual Security Engine is exceeded.

Enhancements in Forcepoint NGFW version 6.4.2

Enhancement	Description
Additional cipher support added	Client and server protection features now support additional ciphers.
Session-Duplicate-Mac situation element	The Session-Duplicate-Mac situation is logged when a different VPN Client user connects using the same MAC address as a VPN Client that is already connected, replacing the previous user.

Enhancements in Forcepoint NGFW version 6.4.4

Enhancement	Description
ECA_Situation-Application-Not-Identified situation element	The ECA_Situation-Application-Not-Identified situation is used when Endpoint Context Agent (ECA) reports an unidentified application.

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 a tunnel interface is configured but not used in a route-based VPN tunnel, OSPF adjacency does not work correctly.	FW	NGFW-10301
When TLS decryption is enabled, the TLS inspection performed by the NGFW Engine does not correctly handle protocol downgrade protection (introduced in TLS 1.3) which causes TLS 1.3 connections to be closed by clients.	FW, IPS, L2FW	NGFW-10874
The dmesg output for the NGFW Engine might include the message "Wrong tuple" when VPN Multi-Link is in use.	FW	NGFW-12249
When an installed policy refers to a TLS Profile that has the option to trust any Certificate Authority enabled, the policy includes all the CAs that have been imported to the Management Server. If any of the CA certificates include fields that are not accepted by the NGFW Engine, the NGFW Engine restarts when the policy is installed.	FW, IPS, L2FW	NGFW-12457

Description	Role	Issue number
When you use Master NGFW Engines and Virtual NGFW Engines, authenticating to the SSL VPN Portal fails. The following message is shown: "Login failed: Internal error: Unable to contact access guardian".	FW	NGFW-12462
When the option "Default Connection Termination in Inspection Policy" is set to "Only Log Connection", connections that match Correlation Situations are terminated.	FW, IPS, L2FW	NGFW-12479
The dynamic routing process restarts when a new interface is added to the configuration at policy installation.	FW	NGFW-12556
When installing a policy, there might be interruptions to traffic if the configuration includes VPN tunnel interfaces that have several IP addresses.	FW	NGFW-12786
When the NGFW Engine is in the IPS or Layer 2 Firewall role, connections that should be terminated due to Correlation Situations might not be terminated.	IPS, L2FW	NGFW-12936
If an interface which has active network traffic is removed when a policy is installed, the NGFW Engine might stop processing traffic.	FW	NGFW-13027
Small TCP segment detection might incorrectly report the TCP_Too-Many-Small-Segments situation when MSS values differ on either side of the NGFW Engine.	FW, IPS, L2FW	NGFW-13129
When moving a Virtual NGFW Engine to another Master NGFW Engine cluster node, the BGP graceful restart option is not enabled.	FW	NGFW-13215
When you enter the <code>vpninfo -o</code> command on the command line of the NGFW Engine, the command does not halt correctly, which causes the VPN process load to increase.	FW	NGFW-13381
When you use a policy-based VPN, the NGFW Engine might start dropping packets after an upgrade. The following message is shown: "New vpn tunnel not resolved [vpn_id[0]=X d_tunnel_id=Y]".	FW	NGFW-13482
Traffic processing performance is lower than expected when the hardware has more CPUs than is allowed by the license for the NGFW Engine. In addition, when you run the <code>sg-status</code> command, errors are shown.	FW, IPS, L2FW	NGFW-13604
After a connection has failed over from one node in a cluster to another, the connection might be discarded. The following message is shown in the Logs view: "Connection dropped due to conflicting rule @X, initially allowed by @0.0". This issue can happen when deep inspection and NAT is applied to the connection.	FW	NGFW-13608
On NGFW appliance models N115 and N335W, up to four SSID Interfaces are supported for the Wireless Interface, but policy installation fails if more than two SSID Interfaces are configured.	FW	NGFW-13715
If you use Multi-Link and you have configured a large number of VPN tunnels, policy installation might fail and the firewall might stop processing traffic.	FW	NGFW-13851

Installation instructions

Use these high-level steps to install the 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/Documentation>.



Note: The sgadmin user is reserved for SMC use on Linux, so it must not exist before the 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 in the Management Client from the **Configuration** view.
- 4) To generate initial configurations, right-click each NGFW Engine, then select **Configuration > Save Initial Configuration**.
Make a note of the one-time password.
- 5) Make the initial connection from the NGFW Engines to the Management Server, then enter the one-time password.
- 6) Create and upload a policy on the NGFW Engines in the Management Client.

Upgrade instructions

Take the following into consideration before upgrading licenses, engines, and clusters.



Note: Upgrading to version 6.4 is only supported from version 6.3 or higher. If you have a lower version, first upgrade to version 6.3.



Note: Starting from Forcepoint NGFW version 6.4, the McAfee Advanced Threat Defense feature is no longer supported. We recommend that you use Forcepoint Advanced Malware Detection instead.

- Forcepoint NGFW version 6.4 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 6.4. See Knowledge Base article [10461](#).

Known issues

For a list of known issues in this product release, see Knowledge Base article [15420](#).

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 <i>disconnect mode</i> 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*

