Next Generation Firewall

Release Notes

6.4.7
Revision A

Contents

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 6.4.7 build version is 20351.

Product binary checksums

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

- sg_engine_6.4.7.20351_x86-64-small.iso

```
SHA1SUM:
6c239796b96e38a14bec55d28c817887e06f9412

SHA256SUM:
7521f3bb0fb449080a5404ccb9f365de3b3d21d1d613dbaa20561bbbd5480505

SHA512SUM:
cca1f3db5e81b412bafbed38aea8b54d
7253eff17548548b7cd727a05a51b800
374ee8f64b86f960e86d5691f971ef15
4d78466aadc8fabb41ca9d87da7cbf41
```

- sg_engine_6.4.7.20351_x86-64-small.zip

```
SHA1SUM:
932f8246cae5a911fe7e3cf85563f60b4a1107f0

SHA256SUM:
22157cf8537e0401ad2e099578369300c23f4662ba718738e768f7f51ffc6cb0

SHA512SUM:
0d31aca364402be60be27f3d820dc37a
73cb12bc47c9a1a4883d50e5845d07c0
9d08d93aef174d2e4dad0dff182ee6dd
db246140b503be04a1ad75443b9b6d69
```

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	The integration of external LDAP servers and Active Directory servers with Forcepoint NGFW has been improved. • 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	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).
Other authentication enhancements	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.

Enhancement	Description
Improvements in application detection	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. **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.
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.

Enhancements in Forcepoint NGFW version 6.4.5

Enhancement	Description
URL filtering queries to the ThreatSeeker Cloud	URL parameters and destination IP addresses are now included in URL filtering queries to the ThreatSeeker Cloud for more precise URL categorization.

Enhancements in Forcepoint NGFW version 6.4.7

Enhancement	Description
Shorter traffic interruption	The length of time for which traffic is interrupted during policy installation or refresh has been shortened.

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
User Responses show N/A as the rule tag variable if the User Responses are triggered by a File Filtering Policy rule that blocks a file type.	FW, IPS, L2FW	NGFW-12311
When traffic from a policy-based VPN is forwarded to the Internet using dynamic source NAT, the central VPN gateway might discard the reply packets if deep inspection is enabled for the traffic.	FW	NGFW-14160
When you change the Tunnel Type for a Route-Based VPN Tunnel from VPN to GRE, the change is not applied in the NGFW Engine configuration.	FW	NGFW-14175
When you add or remove an OSPFv2 Area, PIM restarts.	FW	NGFW-14397
When you add or remove networks in the OSPF configuration, static routes might become inactive.	FW	NGFW-15144
When you use the point-to-point communication mode with OSPF, a host route for the next hop is added even though a subnet is available.	FW	NGFW-15228
Traffic that is forwarded from one VPN to another and also NATed might fail if the Firewall Cluster is in load-balancing mode.	FW	NGFW-15480
When you use TLS inspection, clients must directly trust the CA certificate that has issued the certificate that the NGFW Engine uses to sign the substitute certificates that it generates. TLS inspection does not provide intermediate CA certificates to clients.	FW, IPS, L2FW	NGFW-15825
When you use dynamic routing, removing a self route fails if there is a similar static route.	FW	NGFW-15934
If dynamic routing is configured in an environment with Virtual NGFW Engines, the Master NGFW Engine might restart when you install a policy on multiple Virtual NGFW Engines at the same time.	FW	NGFW-15964
When the route map that is selected as the redistribution filter in a BGP Profile element includes a community, changes to the community setting in the route map are not updated on BGP peers.	FW	NGFW-15992
When you change the OSPF interface type for point-to-point interfaces, the OSPF routing process might restart.	FW	NGFW-16133
Log entries might be sent to the Log Server out of chronological order. Handling the log entries causes an increased load on the Log Server, which can cause the statuses of monitored elements to change rapidly between different status colors.	FW, IPS, L2FW	NGFW-16401
ICMPv6 packets from NGFW Engines that have NAT applied might have incorrect checksums.	FW	NGFW-16424
When you use Google SafeSearch, connection closing is not handled correctly if a DNS server initiates connection closing.	FW	NGFW-16506
Depending on the NGFW appliance model and the original installed NGFW Engine version, some NGFW appliances might lack a swap partition. The lack of a swap partition has no direct impact on the operation of the NGFW Engine.	FW, IPS, L2FW	NGFW-16685

Description	Role	Issue number
In rare cases, the VPN process might restart.	FW	NGFW-16763
A network announced by BGP might be removed from the configuration when additional announced networks are removed.	FW	NGFW-16766
In rare cases, the VPN process might restart when synchronizing IPsec SAs between cluster nodes.	FW	NGFW-17082
In rare cases, refreshing the policy after failover might cause the dynamic routing process to restart.	FW	NGFW-17463
In rare cases when there are a large number of log entries or logs have been spooled on the NGFW Engine, policy installation might fail.	FW, IPS, L2FW	NGFW-17465
When a cluster node is in the locked online state, the node cannot connect to MLC.	FW, IPS, L2FW	NGFW-17467
If connections from the NGFW node itself match rules with SunRPC program numbers, the NGFW Engine might restart.	FW	NGFW-17672
When connections are forwarded to a proxy server, reply packets might be discarded if the NGFW Engine cluster is in load-balancing mode.	FW	NGFW-17826
If a large amount of state synchronization data arrives at the same time, some data might be lost if the recipient UDP buffer gets full.	FW	NGFW-17861
In rare cases, a node in a Master NGFW Engine cluster might become unresponsive during policy installation.	FW	NGFW-18274
If a SIP call issues a re-INVITE for a new related connection, the NGFW Engine might not correctly apply NAT to allow the new connection.	FW	NGFW-18276
When NGFW Engines are running on virtualization platforms that use the vmxnet3 driver, traffic might not be balanced optimally between the available CPUs.	FW, IPS, L2FW	NGFW-18409
The NGFW Engine might restart if SYN flood protection is applied to connections that originate from the NGFW Engine itself.	FW	NGFW-18536
In rare cases, CRL certificate validation might fail.	FW, IPS, L2FW	NGFW-18852
Traffic does not flow correctly when the VPN client uses SSL VPN to connect to a VPN endpoint that is configured on a loopback interface.	FW	NGFW-19629
In rare cases, Master NGFW Engine nodes might restart after a policy is installed if interfaces have been added to the configuration of a Virtual NGFW Engine.	FW	NGFW-19903
This version resolves CVE-2019-6143. Earlier 6.4.x, 6.5.x, and 6.6.x versions have a vulnerability related to the LDAP authentication method. For more information, see Knowledge Base article 17474.	FW	NGFW-20254

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 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 *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*

- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*