Forcepoint

Next Generation Firewall

6.8.5

Release Notes

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 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 https://support.forcepoint.com/ProductSupportLifeCycle.

System requirements

To use this product, your system must meet these basic hardware and software requirements.

CAUTION

To protect the privacy of your data, we recommend using dedicated hardware for all NGFW, SMC, and SMC Appliance installations. For cloud-based virtualization platforms, use an instance type that runs on dedicated hardware. For on-premises virtualization platforms, install the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines. For third-party hardware, do not install any other software on the computer where you install the NGFW Engines or SMC components.

Forcepoint NGFW appliances

We strongly recommend using a pre-installed Forcepoint NGFW appliance for Forcepoint NGFW installations.

Note

Some features are not available for all appliance models. See Knowledge Base article 9743 for appliance-specific software compatibility information.

The majority of the following supported appliances can be used in the Firewall/VPN, IPS, or Layer 2 Firewall role.

- 50 Series (51 and 51 LTE)
- 100 Series (110 and 115) (*Firewall/VPN role only*)
- 120W
- 320 Series (321 and 325)
- 330 Series (330, 331, and 335)
- 1000 Series (1035 and 1065)
- 1100 Series (1101 and 1105)
- 1400 Series (1401 and 1402)
- 2100 Series (2101 and 2105)
- 3207
- 3300 Series (3301 and 3305)
- 3400 Series (3401, 3405, and 3410)
- 5206
- 6205

Note

To use the Forcepoint NGFW Manager, we recommend that you use a Forcepoint NGFW appliance that has at least 4GB of memory.

Basic hardware requirements

You can install Forcepoint NGFW on standard hardware with these basic requirements.

Component	Requirement
CPU	Intel® Pentium D series 2 core or higher
Memory	4 GB RAM
Hard disk	8GB **Note** RAID controllers are not supported.
Peripherals	- DVD drive - VGA-compatible display - Keyboard
Interfaces	- One or more network interfaces for the Firewall/VPN role - Two or more network interfaces for the IPS in IDS configuration - Three or more network interfaces for inline IPS engine or Layer 2 Firewall For information about supported Ethernet interface types and adapters, 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 NGFW 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.

Component	Requirement
CPU	Intel® Pentium D series 2 core or higher
Memory	4 GB RAM
Virtual disk space	8 GB
Hypervisor	One of the following: - VMware ESXi 6.5 or 6.7 - KVM with Red Hat Enterprise Linux 7.8 or 8.1 - (Firewall/VPN role only) Microsoft Hyper-V on Windows Server 2012 R2 or Windows Server 2016 with an Intel 64-bit processor
Interfaces	- At least one virtual network interface for the Firewall/VPN role - Three virtual network interfaces 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 number and checksums

The build number for Forcepoint NGFW 6.8.5 is 24304.

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

- sg_engine_6.8.5.24304_x86-64-small.iso

```
SHA1SUM:
3815caf9a26c894b1a3d7f092292ee29d7a9f307

SHA256SUM:
d15024c5bfabb7792af8093a93db9ebdb52c254858692d4d4f5881facc5fa7d8

SHA512SUM:
e8f897dd2ae53295b76cd0ff5ccd6625
a8b79e383289d8ef0029bf6a539e7458
a8f92b5c0bbaa1c809a0ca34d058c48b
a8e9878446d960702253578dfd275e20
```

- sg_engine_6.8.5.24304_x86-64-small.zip

```
SHA1SUM:
775c1100b84784bd993e7f7bd8ddac5abc9ddd56

SHA256SUM:
961c1ece9b9e9e34db9a28ab172413a3068410099c65cd46cceb937e433677b1

SHA512SUM:
3870d42b68a084b0b0b49d0c308f6c1a
279c707684f83eab9dd4df52431dc8ae
33bd44520f1bac51be0f42612dacd890
4622d3cfe7aa2e282457152d5651ea18
```

Compatibility

Forcepoint NGFW 6.8 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.8 or higher
- Dynamic Update 1247 or higher
- Forcepoint VPN Client for Windows 6.6.0 or higher
- Stonesoft VPN Client for Windows 6.1.0 or higher
- Forcepoint VPN Client for Mac OS X 2.0.0 or higher
- Forcepoint VPN Client for Android 2.0.0 or higher
- Server Pool Monitoring Agent 4.0.0 or higher

- Forcepoint Endpoint Context Agent (ECA) 1.4.0 or higher
- Forcepoint Endpoint Context Agent (ECA) included in Forcepoint One Endpoint 19.05 or higher
- Forcepoint User ID Service 1.1.0 or higher

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*.

Easier configuration of dynamic link selection for NGFW Engines

It is now possible to select Link Usage Profile elements for NGFW Engines in the Firewall/VPN role to define which link types are preferred, avoided, or not used for specific types of outbound Multi-Link traffic. NGFW Engine-specific exceptions to the Link Usage Profile also allow you to specify which traffic uses specific NetLinks.

PPPoE support on VLAN interfaces

You can now configure point-to-point protocol over Ethernet (PPPoE) for dynamic IP addresses that are assigned to VLAN interfaces. Using PPPoE for dynamic IP addresses that are assigned to VLAN interfaces allows you to connect to an ISP line that uses 802.1q VLAN tagging without using a separate switch.

Re-authentication when using browser-based user authentication

If an end user has authenticated using browser-based user authentication and the session will soon expire, the user can re-authenticate to extend the authentication time-out and avoid connections closing before the user has finished their tasks.

Dynamic update packages in the NGFW Manager

You can now upload and activate dynamic update packages in the NGFW Manager. Dynamic update packages provide updates for NGFW Engines, especially for deep inspection features.

For example, new threat patterns and changes in the system Templates and Policies are introduced in dynamic updates for up-to-date detection. They can also revise the default elements you use to configure the system.

For more information, see the *Forcepoint NGFW Manager and VPN Broker Product Guide*.

Support for the NGFW Engine tester in the NGFW Manager

You can now use the NGFW Engine tester in the NGFW Manager. The NGFW Engine tester runs various checks on the NGFW Engine and initiates responses based on the success or failure of these tests.

For more information, see the *Forcepoint NGFW Manager and VPN Broker Product Guide*.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 6.8.0

Enhancement	Description
Custom script upload for NGFW Engines when using Custom Properties Profile elements	To upload custom scripts to the NGFW Engine, you can add the scripts to the properties of the NGFW Engine using a Custom Properties Profile element. The scripts are uploaded when the policy is installed or refreshed.
Expiration time for one-time passwords	You can now set the expiration time for one-time passwords that are generated when you save the initial configuration for an NGFW Engine. If the one-time password is not used, it automatically expires after the expiration time has elapsed. By default, one-time passwords expire after 30 days.
User domain support for integrated ICAP servers for DLP	NGFW integration with external ICAP servers for DLP now uses the WinNT schema in the X-Authenticated-Users header instead of the Local schema that was used previously. Using the WinNT schema allows matching users against a user domain in the user directory on the ICAP server.
Significant improvements in inspection performance	There are general improvements in how the NGFW Engines inspect traffic. Inspection performance has improved significantly, especially when application detection is enabled.
VPN broker member synchronization in VPN Broker high availability environment	When you use the VPN Broker in a high availability (HA) environment, the changes you make to the list of VPN Broker members are automatically synchronized with all the other VPN Broker gateways in the NGFW Manager.
ACPI shutdown support	Support for advanced configuration and power interface (ACPI) shutdown has been implemented. This feature allows graceful shutdown when terminating virtual instances in the Microsoft Azure and Amazon Web Services platforms.

Enhancements in Forcepoint NGFW version 6.8.1

Enhancement	Description
Improved VPN performance	VPN performance has been improved in environments where there is a high rate of new VPN connections.

Enhancements in Forcepoint NGFW version 6.8.4

Enhancement	Description
More memory usage details available using SNMP Agents for NGFW Engines	Two new counters for available memory are now reported in Forcepoint NGFW-specific SNMP MIBs. The new OIDs are fwMemBytesAvailable and fwMemBytesSReclaimable. To use the new counters, update the NGFW-specific SNMP MIB for your SNMP tools to the NGFW MIB 6.9 level. For more information, see Knowledge Base article 19210.

Enhancements in Forcepoint NGFW version 6.8.5

Enhancement	Description
Detections of brute force attacks against NGFW user authentication	After you install dynamic update package 1303 or higher, you can use new Correlation Situation elements to detect and prevent brute force attacks against NGFW user authentication. For more information, see Knowledge Base article 19259.

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.

The **Role** column indicates the NGFW Engine roles that are affected by the issue:

- FW — Firewall/VPN
- IPS — IPS
- L2FW — Layer 2 Firewall
- VPN Broker — VPN Broker gateway

To resolve the issue, upgrade NGFW Engines that have the specified roles.

Description	Role	Issue number
The internal DHCP server on NGFW Engine interfaces might stop working over time.	FW	NGFW-4947
When you use Network Application elements as matching criteria in access rules, many log entries with the Connection_Rematched situation might be generated before log entries with the Connection_Allowed or Connection_Discarded situation. Log entries with the Connection_Rematched situation should only appear when the Inspection Diagnostics option is enabled.	FW, IPS, L2FW	NGFW-21803
When you remove the probing method for route monitoring from a route, the route itself is also removed.	FW	NGFW-22172
When the same VPN Broker Gateway is used in more than one VPN Broker Domain, policy installation fails when you publish the configuration in the NGFW Manager.	VPN Broker	NGFW-23679
The SSL VPN monitoring view for Firewall Clusters might not show all connected users.	FW	NGFW-26519

Description	Role	Issue number
The NGFW Engine does not interpret CA certificates that use the RSASSA-PSS signature algorithm. As a result, policy installation fails.	FW, IPS, L2FW	NGFW-27677
When there is a very large VPN configuration, the VPN process might restart during policy installation.	FW	NGFW-28723
When route probing is configured for an interface that has a dynamic IP address, but the interface does not receive an IP address, the NGFW Engine might restart during policy installation.	FW	NGFW-29257
After an NGFW Engine has been connected to a backup Log Server, the NGFW Engine only tries to use the first defined contact address of the primary Log Server to reconnect to it. If that IP address is unreachable, the NGFW Engine never reconnects to the primary Log Server.	FW, IPS, L2FW	NGFW-29288
When you use Forcepoint User ID Service, nested groups are added with the user’s domain even if the nested groups are from a different subdomain than the user’s domain or from the parent domain.	FW, IPS, L2FW	NGFW-29537
In rare cases, when a VPN configuration change is applied and there is traffic that matches the VPN, the NGFW Engine might restart during policy installation.	FW	NGFW-30131
TLS decryption might fail for some connections in Chrome version 86 or newer, and Microsoft Edge. When the browser attempts to resume a TLS session using the session ticket, the NGFW Engine fails to modify the server stream for decryption.	FW, IPS, L2FW	NGFW-30222
When a configuration update from the VPN Broker to a VPN Broker Member fails, future configuration updates might also be prevented.	VPN Broker	NGFW-30298
After VPN rekeying, a node in a Firewall Cluster might continue using the old security parameter index (SPI).	FW	NGFW-30387
In rare cases, when you use round trip time as the method for outbound load balancing and you use application routing, the NGFW Engine might restart.	FW	NGFW-30401
In an environment with Master NGFW Engines and Virtual NGFW Engines, OSPF might be unstable if there are a large number of neighbors.	FW	NGFW-30419
Rules that have Zone elements as matching criteria in the destination cell do not work on VLAN interfaces that have PPPoE enabled.	FW	NGFW-30431
On Firewall Clusters, SIP calls might be terminated if they are not answered in 32 seconds.	FW	NGFW-30480
If the state of some nodes in a Firewall Cluster changes between online, offline, or standby while the routes for dynamic routing are being synchronized, some dynamic routes might be lost from the dynamic routing configuration.	FW	NGFW-30492
You cannot use the VPN Broker on a Master NGFW Engine cluster that has only one node.	VPN Broker	NGFW-30632
Log entries generated by rules with the discard action are not compressed even though log compression is enabled in the logging options for the rules.	FW, IPS, L2FW	NGFW-30702
DHCP relay might be slow to forward DHCP requests if there are a large number of DHCP requests.	FW	NGFW-30734
Due to file access permissions, HTTPS services for the SSL VPN Portal might show a "service not available" error.	FW	NGFW-30787

Description	Role	Issue number
When a user response is triggered for HTTPS connections, the user response might not be sent using the trusted certificate from the Client Protection Certificate Authority that is used to decrypt the connection.	FW, IPS, L2FW	NGFW-30836
Policy installation might fail on the VPN Broker when the allowed networks for a VPN Broker Member include ANY.	VPN Broker	NGFW-30837
Communication between Virtual NGFW Engines on the same Master NGFW Engine interface might fail if the physical interface uses the i40e driver.	FW	NGFW-30870
Dynamic routing has been optimized to work faster with a large number of announced networks and prefix lists.	FW	NGFW-30929
When you modify a VPN site in a mobile VPN that has SSL VPN tunnels and refresh the policy, all VPN Client users are disconnected to force them to reconnect and receive the new VPN configuration. If many VPN Client connections are active when the policy is refreshed, the Firewall nodes that are handling the VPN connections might restart, causing the policy installation to fail.	FW	NGFW-30963
When you use a loopback IP address as a VPN endpoint, sending traffic to the VPN tunnel fails.	FW	NGFW-30970
In rare cases, the inspection process might restart.	FW, IPS, L2FW	NGFW-31012
When log data is spooled on an NGFW Engine, sending log data becomes slower the more files there are to send. As a result, NGFW Engine nodes might intermittently appear gray in status monitoring views when the log spool is cleared.	FW, IPS, L2FW	NGFW-31021
In rare cases when session limiting is used, the NGFW Engine might restart.	FW, IPS, L2FW	NGFW-31131
Dnsmasq has been updated to address CVE-2020-25681, CVE-2020-25682, CVE-2020-25683, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686 and CVE-2020-25687.	FW	NGFW-31270
Sudo has been updated to address CVE-2021-3156.	FW, IPS, L2FW	NGFW-31339
In large VPN configurations with many different remote VPN endpoints, traffic might be briefly interrupted during policy installation.	FW	NGFW-31352

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, NGFW Engines, and clusters.

Note

Upgrading to version 6.8 is only supported from version 6.5 or higher. If you have a lower version, first upgrade to version 6.5.

Note

If you use safe search features in NGFW 6.6 or lower, you must refresh the policy on the NGFW Engine cluster after all the members of the cluster have been upgraded to NGFW 6.7 or higher. Otherwise, safe search might not work correctly after the upgrade.

- Forcepoint NGFW version 6.8 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 NGFW 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*.

Known issues

For a list of known issues in this product release, see Knowledge Base article 18382.

Known limitations

This release of the product includes these known limitations.

Limitation	Description
Inspection in asymmetrically routed networks	In asymmetrically routed networks, using stream-modifying features such as TLS Inspection, URL filtering, and file filtering can make connections stall.
Inline Interface disconnect mode	The disconnect mode for Inline Interfaces is supported only on modular appliance models that have full-sized bypass interface modules (not mini 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, release notes, Knowledge Base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint support website. If you do not yet have credentials, create a customer account. See https://support.forcepoint.com/CreateAccount.

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*

© 2021 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
Published 11 February 2021