Forcepoint

Next Generation Firewall

6.8.6

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 6.8.6 is 24355.

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

- sg_engine_6.8.6.24355_x86-64-small.iso

```
SHA1SUM:
f6ce50be2aa5575ea865463264516b6be843120d

SHA256SUM:
94bf7bdb620e00f766f1f5e0265cb5648f34f00118480244eff6cd51d53fe97d

SHA512SUM:
c0482b4c7d1a5d6f0321c541ec2dd159
5e0dc71e090c6bb570a8ba462997bd3b
597bf9b4432390f6fbf98ff1d7cc8873
7b54c4001e9121cb6feb44c61dfd1172
```

- sg_engine_6.8.6.24355_x86-64-small.zip

```
SHA1SUM:
22a3d425172eafab3893c586957b1e9bbf11caaf

SHA256SUM:
a24169c9d4180a28dfa2d8d4db7cf660d6c229c7e7ebb629ced4ef48afe1c6ba

SHA512SUM:
99c746a6d7d23dd6ecf004ccaf29ed88
36eafc2bd07525cc6b5eb0a920cb3d41
adaf902f93fc20e67b5671dc4a323daf
ad8f8e1df24efd822700a9d7a30810bb
```

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.

Enhancements in Forcepoint NGFW version 6.8.6

Enhancement	Description
Configuration of bidirectional forwarding detection using the Management Client	Forcepoint NGFW Engine previously supported the configuration of bidirectional forwarding detection (BFD) using command line tools on the NGFW Engine. You can now configure BFD using the Management Client. When you use the BGP protocol for dynamic routing, you can optionally use BFD to detect neighbor failures. The NGFW Engine sends packets at the specified interval and waits for a reply. If the NGFW Engine does not receive a reply within the specified length of time, the neighbor is considered to have failed.
TLS inspection for server protection allows TLS handshake downgrade	When you use TLS inspection for server protection without configuring client protection, the certificate authority (CA) can now downgrade unsupported cipher suites, extensions, or ALPN protocols for TLS.
Improved performance of interface driver for virtualization platforms	The performance of the vmxnet3 interface driver for virtualization platforms has been improved.

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
When TLS decryption and certificate revocation checks are enabled, HTTPS connections might might be terminated by the TLS_Unrecoverable-Error situation.	FW, IPS, L2FW	NGFW-22560
In Access rules in the Firewall policy that match user information retrieved from Forcepoint User Identification Service (FUID) or Integrated User Identification Service (IUID), you can only use Active Directory security groups as user groups. You cannot use Active Directory organizational units as user groups.	FW, IPS, L2FW	NGFW-22878
When a trusted CA certificate expires but there is another valid trusted CA certificate that uses the same subject and public key, TLS inspection might fail to validate the server certificate chain.	FW, IPS, L2FW	NGFW-24525
In mobile VPNs that use SSL VPN tunnels, VPN Clients might fail to receive virtual IP addresses from a firewall cluster when previous connections have not been closed explicitly.	FW	NGFW-29302
When incoming packets from VPNs do not match the traffic selectors of the negotiated IPsec SA, a log entry is not generated. The following message is shown in other log entries: "SA selector mismatch after decapsulation".	FW	NGFW-30291
When the NGFW Engine is behind specific third-party NAT devices, NetLink probing might stop working until the NGFW Engine is restarted.	FW	NGFW-30378
If the Users monitoring view is open, users that have logged off are not removed from user monitoring.	FW	NGFW-30659
When a backup Log Server is configured, route monitoring might not work.	FW	NGFW-31276
Memory usage for the VPN process might increase and cause the VPN to stop working or policy installation to fail. This issue especially affects NGFW Engine nodes that are in the offline or standby state.	FW	NGFW-31353
When there is an attempt to open a related connection for SIP, the inspection process might restart.	FW	NGFW-31674
If you have configured multiple DNS servers and the NGFW Engine uses different interfaces to contact each DNS server, DNS relay might not work.	FW	NGFW-31787
The FTP protocol agent might not work correctly in strict mode without inspection when the following FTP commands are used: PRET, HOST, CLNT, RANG, or HASH.	FW	NGFW-31837
When you move a Virtual Resource to an interface that is shared by multiple Virtual NGFW Engines, Virtual NGFW Engine interfaces lose their IP addresses when you install a policy.	FW, IPS, L2FW	NGFW-31972
Policy routes do not work on VPN Broker Members.	FW	NGFW-32055
When you use TLS inspection and the destination server uses a self-signed certificate, users are not prompted to trust the server certificate.	FW, IPS, L2FW	NGFW-32117
The TCP_Segment-SYN-Options-Conflict packet validation situation might drop packets without logging.	FW, IPS, L2FW	NGFW-32148
When Virtual NGFW Engines that use the same shared interface are active on different Master NGFW Engine nodes, routing traffic from one Virtual NGFW Engine to another through the shared interface fails.	FW	NGFW-32415

Description	Role	Issue number
Interface monitoring in the Management Client might not correctly show the status of the VPN Broker interface.	FW	NGFW-32457
After a Virtual NGFW Engine has been removed from a Master NGFW Engine, policy installation might cause the NGFW Engine to restart if the removed Virtual NGFW Engines is included in the VPN configuration.	FW	NGFW-32477
Using the SSL VPN Portal to access services does not work when you use asynchronous HTTP requests.	FW	NGFW-32513
When you use outbound load-balancing and forward traffic to a proxy service for inspection, TCP retransmission packets are not handled correctly.	FW	NGFW-32571
In rare cases, the NGFW Engine might restart when NAT-T is used for VPN traffic.	FW	NGFW-32577
When the NGFW Engine is configured to listen on over 50 interfaces for browser-based user authentication, the NGFW Engine might restart during policy installation.	FW	NGFW-32585
When you use route-based VPNs with dynamic routing and there are a large number of interfaces that have dynamic IP addresses, policy installation might be slow. While the dynamic routing process is updating the configuration, VPN communication might be stopped.	FW	NGFW-32664
When the VPN Broker Gateway receives new information about VPN Broker Members, it does not receive information about the tunnel mode of the remote VPN Broker Members.	VPN Broker	NGFW-32694
When a user belongs to hundreds of groups, VPN Client connections to SSL VPN gateways might stop progressing when they reach the authentication phase.	FW	NGFW-32713
DNS relay does not process incoming TCP DNS requests that arrive on interfaces other than the interface that has a listening IP address for DNS relay configured.	FW	NGFW-32797
In rare cases when application routing is used, the timing of the NAT processing during policy installation might cause the NGFW Engine to restart.	FW	NGFW-32886
It is not possible to replicate SMC administrator accounts that include a dash (-) in the name to NGFW Engines.	FW, IPS, L2FW	NGFW-32971
When you use Master NGFW Engines and Virtual NGFW Engines, synchronizing a large number of routes for dynamic routing on multiple Virtual NGFW Engines might not always work.	FW	NGFW-32988
In rare cases, inspection of SMB traffic can cause the inspection process to run out of memory.	FW, IPS, L2FW	NGFW-33007
The SSL VPN Portal might not be able to parse cookie headers correctly for a service.	FW	NGFW-33019
When you change the route metric for a static IPv6 route, the NGFW Engine might restart during policy installation.	FW	NGFW-33088
Multipath ECMP routes are not added to dynamic routing.	FW	NGFW-33090
Nodes that are in the lock online state do not send dynamic route synchronization to other nodes.	FW	NGFW-33091
When application routing is defined in the NAT rules, specific types of TCP packets can cause the inspection process to restart.	FW	NGFW-33143

Description	Role	Issue number
During policy installation, the processing of VPN traffic might be interrupted for up to 5 seconds when you use the VPN Broker or when VPN traffic is forwarded from one VPN tunnel to another.	FW	NGFW-33201
The validation of source IP addresses and remote identities might be too strict in IKE negotiations between VPN Broker Members.	FW, VPN Broker	NGFW-33260
The VPN Broker Gateway might be too busy to send monitoring updates when a large number of VPN Broker Members are connected to it.	VPN Broker	NGFW-33336
A VPN Broker Member might update its VPN configuration when it receives an update from the VPN Broker Gateway even though the configuration has not changed.	FW	NGFW-33466
When a VPN is configured, memory usage on NGFW Engine cluster nodes that are in the offline or standby states might increase over time. Eventually, the nodes stop working.	FW	NGFW-33474
If the configuration includes a large number of interfaces, the NGFW Engine might restart during policy installation.	FW, IPS, L2FW	NGFW-33510
A problem with the inspection process might cause the NGFW Engine to restart.	FW, IPS, L2FW	NGFW-33512
When many external VPN gateways that have dynamic IP addresses have the same local endpoint IP address, VPN monitoring traffic for different tunnels might be incorrectly routed to the wrong tunnel.	FW	NGFW-33736
Using the avdbfetch command to manually download the anti-malware database does not work as described in KB36197.	FW, IPS, L2FW	NGFW-33868

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.

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

In the Forcepoint Customer Hub, 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 in the Forcepoint Customer Hub 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 Customer Hub. 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*

Published 21 June 2021