Forcepoint

Next Generation Firewall

6.5.9

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.

- 100 Series (110 and 115) (*Firewall/VPN role only*)
- 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)
- 3200 Series (3202, 3206, and 3207)
- 3300 Series (3301 and 3305)
- 5206
- 6205

Sidewinder S-series appliances

The following appliance models can be re-imaged to run Forcepoint NGFW software in the Firewall/VPN role.

- S-1104
- S-2008
- S-3008
- S-4016
- S-5032
- S-6032

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 6.0 and 6.5 ■ KVM (KVM is tested as shipped with Red Hat Enterprise Linux Server 7.4 and 7.5) ■ Microsoft Hyper-V on Windows Server 2012 or Windows Server 2016 Firewall/VPN role only. An Intel 64-bit processor is required.
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 6.5.9 is 21503.

Use checksums to make sure that files downloaded correctly.

- sg_engine_6.5.9.21503_x86-64-small.iso

```
SHA1SUM:
521e35a05a414611f8897b6c2996d83371162236

SHA256SUM:
072d698b75ff96ba311a345d0c7143baf4cd6a49ef249310db19809424394898

SHA512SUM:
13f3062fb426a36d79625babecbc59bf
e67ee430c550d3e70939eaff2e181c54
9ef6c1dfd8aaf7a0227ee57a8a3a06cf
6d050ae8fb1557b246c3901e9f70c181
```

- sg_engine_6.5.9.21503_x86-64-small.zip

```
SHA1SUM:
8c3606c552876d6d5763c402d90900f7f9811d2e

SHA256SUM:
f873d081b57df0f75318bd150b2999c0b06fdda7741911cc631b83c3920af1e0

SHA512SUM:
b0092faffcc22257861f3642d072b63c
809cb2d966f4fd61b786d186fa5fc398
9f382997b6eebbbe43b5013645d9ca35
5a27861848c3eee275cf3677ea09aa32
```

Compatibility

Forcepoint NGFW 6.5 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.5 or higher
- Dynamic Update 1104 or higher
- Stonesoft® VPN Client for Windows 6.1.0 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

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*.

SD-WAN dashboard

The SD-WAN dashboard makes the software-defined wide area network (SD-WAN) features that are already part of Forcepoint NGFW more visible. The SD-WAN dashboard allows you to monitor SD-WAN features, such as outbound Multi-Link and Multi-Link VPNs, and to view statistics and reports related to SD-WAN features.

Application routing

You can now apply different NAT rules to traffic, select which VPN traffic uses, and redirect traffic to different proxy servers depending on the network applications detected in the traffic.

Route metrics, ECMP, and route monitoring

You can now define multiple static routes to the same destination and apply metrics to the routes. The routes with a lower metric value can be used as backup routes. When you enable the equal-cost multi-path (ECMP) feature on the routes, there is a potential increase in bandwidth as traffic is balanced between the routes. In addition, you can use probes to monitor the status of a route. If a route is unavailable, the route is removed from the routing table and traffic is automatically sent over another route.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 6.5.0

Enhancement	Description
Integrated User ID Service on NGFW Engines	You can now use the Integrated User ID Service on the NGFW Engines to provide transparent user identification for access control by user. The Integrated User ID Service is primarily meant for demonstration purposes and proof-of-concept testing of user identification services.
LDAP authentication for administrators	You can now authenticate administrators using simple password authentication against integrated external LDAP databases.

Enhancement	Description
VPN tunnels can remain established	You can now set specific VPN tunnels to always remain established even when no traffic is sent through the VPN tunnel.
IPv6 support for DHCP relay	You can now use DHCP relay on interfaces that have IPv6 addresses.
Node-initiated contact to Management Server for clustered NGFW Engines	Firewall Clusters and Master NGFW Engines in the Firewall/VPN role now support node-initiated contact to the Management Server. The clustered NGFW Engine opens a connection to the Management Server and maintains connectivity.
More precise controls for endpoint use	You can now define which VPN endpoints can communicate with each other, and how the endpoints are used in a Multi-Link configuration.
Dynamic routing with active-active clustering	You can now use dynamic routing in Firewall Clusters that use load-balancing mode. In load-balancing mode, all nodes in the cluster are online at the same time and traffic is balanced between the nodes, increasing performance for inspection and VPN traffic.
Dynamic elements specific to cloud platforms	You can use a specific naming scheme with Domain Name elements in Access rules to run a script on the NGFW Engine that resolves dynamic element names specific to a cloud platform to IP addresses. The IP addresses are resolved through API calls rather than regular network DNS queries. For more information, see Knowledge Base article 16290.
Update to using IKEv1 and certificate-based authentication	Previously, the NGFW Engine used the CA IssuerName in the IKE payload of the certificate request during IKEv1 negotiation. Starting from NGFW 6.5, the SubjectName is used in the payload, as recommended in RFC 4945.

Enhancements in Forcepoint NGFW version 6.5.1

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.
More precise URL categorization	URL parameters and destination IP addresses are now included in URL filtering queries to the ThreatSeeker Cloud for more precise URL categorization.
Faster policy installation	Policy installation is now faster for configurations that include a larger number of interfaces and changes to networks.

Enhancements in Forcepoint NGFW version 6.5.2

Enhancement	Description
Shorter traffic interruption	The length of time for which traffic is interrupted during policy installation or refresh has been shortened.
Faster synchronization of dynamic routing tables	Synchronizing very large dynamic routing tables is now faster. With a large dynamic routing table, the non-active dynamic routing node receives changes more reliably.

Enhancements in Forcepoint NGFW version 6.5.5

Enhancement	Description
New syntax for CN field in certificate requests for browser-based user authentication	It is now possible to use a specific syntax for the CN field in a certificate request (CSR) for browser-based user authentication so that the Subject Alternative Name (SAN) fields can already be defined when the NGFW Engine generates the certificate request for browser-based user authentication. For more information, see Knowledge Base article 17375.

Enhancements in Forcepoint NGFW version 6.5.6

Enhancement	Description
Support for YouTube in DNS-based SafeSearch	DNS-based SafeSearch has been extended to support YouTube.

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
In NGFW Engine clusters, when an interface that has DHCP relay enabled is also selected as the Default IP Address for Outgoing Traffic, DHCP requests might go out through the incorrect interface if there are interfaces without NDI addresses.	FW	NGFW-2657
Power supply monitoring for NGFW appliances might trigger an alert even though the status of the power supply is OK.	FW, IPS, L2FW	NGFW-25942
Error messages about the connection to sandbox servers refer to a cloud connection even when you use an on-premises local sandbox.	FW, IPS, L2FW	NGFW-26013
Compressed logs with the Log_Compress-SIDs situation do not include rule tags.	FW, IPS, L2FW	NGFW-26597
When you use Virtual NGFW Engines on NGFW Appliances with limited RAM, policy installation might fail if policies that include different dynamic update packages are installed on different Virtual NGFW Engines.	FW, IPS, L2FW	NGFW-27435
When the NGFW Engine is inspecting a TCP connection that has inconsistent sequence numbers, the inspection process might restart. Capture interfaces are most likely to receive packets that have inconsistent sequence numbers.	FW, IPS, L2FW	NGFW-27633
When there are large bursts of user group membership updates in ECA, ECA state sync might log the following error: "Resource temporarily unavailable State sync internal communication error".	FW, IPS, L2FW	NGFW-27679
When the NGFW Engine is handling SIP UDP traffic, the inspection process might restart.	FW, IPS, L2FW	NGFW-27725
When you use the multicast MAC clustering mode, nodes incorrectly reply to ARP requests about CVI addresses.	FW	NGFW-28019
SNMP monitoring for VPN SAs always returns 0 as the value.	FW	NGFW-28392

Description	Role	Issue number
In rare cases, the node might go offline because dynamic routing uses too much memory.	FW	NGFW-28542
When the NGFW Engine initiates reset packets for traffic that uses a VPN, the NGFW Engine might not correctly send the reset packets.	FW	NGFW-28595
When you use the ratio-based load-balancing method for outbound Multi-Link, monitoring views in the Management Client do no show the number of concurrent connections that are currently using the outbound Multi-Link.	FW	NGFW-28718
When you modify a large VPN configuration, policy installation might take too long and the VPN process might restart.	FW	NGFW-28887
ICMP ID is used to monitor external VPN endpoints. If you use load balancing clustering, ICMP echo replies from remote endpoints might be discarded.	FW	NGFW-28940

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 6.5 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 6.5 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*.
- 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 NGFW Engine to Forcepoint NGFW version 6.5. See Knowledge Base article 10461.

Known issues

For a list of known issues in this product release, see Knowledge Base article 16287.

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

© 2020 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 29 September 2020