FORCEPOINT

Next Generation Firewall

Release Notes

6.5.1

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)
- 300 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 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 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

Component	Requirement
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 7.1 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.
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 6.5.1 is 21108.

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

- sg_engine_6.5.1.21108_x86-64-small.iso

```
SHA1SUM:
8c6545c10bcd8875061fae9355f2a88de3050460

SHA256SUM:
d00cd28653f7feee0ec530b6f3c1ddb395346972f56c32b5042145e527658058

SHA512SUM:
68049d3253c4d1f6839b2e5b2720d6a6
7d3710ad3f5f0a97ead8f36ce5e398ba
c4ba323c41f039732428f52a814fed79
4a438c7d8a1370615c790610a37b971d
```

- sg_engine_6.5.1.21108_x86-64-small.zip

```
SHA1SUM:
40a2f35088f35c1e88f4211567a8e5cc735a5a34

SHA256SUM:
095afd70a71a908e8476efc659e39e366a017445e849279928b770cb37a76132

SHA512SUM:
98fd7d576b88b2dcb6b3e23ab621069e
183cd46453034f7cb58a80662dc18fcd
b26bc0ea6d9c9fb70092b8a32f401236
9b77ceaf79cc42780dc19434b7e00983
```

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.
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.

Enhancement	Description
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.

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
The User Domain log field does not always contain information for connections related to the SSL VPN Portal.	FW	NGFW-10634
If "Enforce Google SafeSearch" is set to "On" in the Protocol Parameters of a custom duplicate of the SSM DNS Proxy (UDP) Service, the NGFW Engine might restart when traffic matches a rule that contains the custom Service element.	FW	NGFW-12001

Description	Role	Issue number
When the option "Default Connection Termination in Inspection Policy" is set to "Only Log Connection", connections that match Correlation Situations are terminated.	FW, IPS, L2FW	NGFW-12479
When you use URL Categories or Network Applications in the policy to allow TLS traffic, traffic might not be decrypted as intended if a later rule has Decryption: Disallowed selected in the action options.	FW, IPS, L2FW	NGFW-12565
When a connection is logged by the inspection facility, Connection_Closed log entries do not include user information.	FW, IPS, L2FW	NGFW-12868
When the NGFW Engine is in the IPS or Layer 2 Firewall role, connections that should be terminated due to Correlation Situations might not be terminated.	IPS, L2FW	NGFW-12936
When deep inspection is enabled for a connection, possible allowed ICMP error messages that refer to the original inspected connection are not logged.	FW, IPS, L2FW	NGFW-13082
When you specify QoS classes for Network Applications, QoS exceptions in Multi-Link VPNs might not work as expected.	FW	NGFW-13376
When you use a policy-based VPN, the NGFW Engine might start dropping packets after an upgrade. The following message is shown: "New vpn tunnel not resolved [vpn_id[0]=X old_tunnel_id=Y]".	FW	NGFW-13482
Logging of dynamic routing diagnostics for PIM might be excessive.	FW	NGFW-13646
When you use dynamic routing with a firewall cluster in balancing mode, specific packets related to dynamic routing might be dropped. When the state of cluster nodes changes, dynamic routing might not run reliably.	FW	NGFW-13811
When you use TLS inspection and certificate revocation checks are enabled, connections to some websites might fail.	FW, IPS, L2FW	NGFW-13873
The ISP Link is not consistently logged for all connections that match NAT rules for outbound traffic management. As a result, overviews and reports that contain statistics about traffic by ISP Link might be missing part of the traffic.	FW	NGFW-14151
When a tunnel interface has both a CVI and an NDI, and the route-based VPN has tunnels of the type VPN or GRE, dynamic routing through the route-based VPN fails.	FW	NGFW-14177
When deep inspection is enabled for HTTPS traffic, the performance of Virtual NGFW Engines decreases.	FW, IPS, L2FW	NGFW-14217
The SIP Protocol Agent only recognizes the phone and ip tokens in the user parameters. The SIP Protocol Agent does not recognize the other-user token in the user parameters. SIP headers that include other-user tokens are not processed.	FW, IPS, L2FW	NGFW-14314
In rare cases, when a TCP connection directed to the node itself is blocked with the Refuse action, the NGFW Engine might restart.	FW, IPS, L2FW	NGFW-14382
When the NGFW Engine processes certain types of MSRPC traffic, the NGFW Engine might write excessively to the console, which can degrade the performance of the engine. As a result, traffic handling might be interrupted, and the NGFW Engine node might go offline.	FW, IPS, L2FW	NGFW-14392
When one or more nodes in a firewall cluster in balancing mode is offline, the Tunnels status card in the SD-WAN dashboard shows 66% health for tunnels to third-party gateways.	FW	NGFW-14472

Description	Role	Issue number
The SD-WAN dashboard might randomly show packet loss for tunnels that are idle.	FW	NGFW-14495
When you use Endpoint Application and Endpoint Settings elements for ECA in an Access rule without enabling deep inspection, a later rule that allows FTP traffic does not allow the related data connections for FTP.	FW, IPS, L2FW	NGFW-14679
When you use certificate revocation status checking, some failures in processing CRLs are not correctly handled. As a result, certificate validation might stop working, and the certmand process might cause a high CPU load on the NGFW Engine. The NGFW Engine might stop processing TLS-related traffic.	FW, IPS, L2FW	NGFW-14729
When you install a policy that includes changes to the network configuration, processing of dispatched traffic in a firewall cluster stops for longer than expected.	FW	NGFW-14824
When RADIUS authentication is configured to require multiple Access-Challenge responses, browser-based user authentication does not correctly request the second challenge response.	FW	NGFW-14840
When a connection might potentially match more than one Access rule based on the payload of the connection, logging options from an earlier potentially matching rule might be applied even though a later rule with different options actually allowed the connection.	FW, IPS, L2FW	NGFW-14849
When a connection might potentially match more than one Access rule based on the payload of the connection, and the first potentially matching rule includes the HTTPS Service with the "HTTPS decryption and inspection" parameter set to "No", using the HTTPS Service with the "HTTPS decryption and inspection" parameter set to "Yes" in a later rule does not enable decryption.	FW, IPS, L2FW	NGFW-14947
When there is a VPN configured and the connectivity status of interfaces changes rapidly, the NGFW Engine prints a large number of messages about failing routing to the console. The large number of messages can cause other symptoms, such as interrupting the heartbeat connection in clusters.	FW	NGFW-15020
If the ECA Client sends partial user information to the NGFW Engine, the connection from the ECA Client is dropped. The following information message is shown in the logs: "Connection severed: CORRUPTION".	FW, IPS, L2FW	NGFW-15035
When you add or remove networks in the OSPF configuration, static routes might become inactive.	FW	NGFW-15144
When the User Domain defined in the Management Client does not match the DNS name of the user domain, log entries generated by the ECA_metadata_login Situation contain a different User Domain than log entries generated by the Access rules.	FW, IPS, L2FW	NGFW-15156
Google SafeSearch might not work when dynamic source NAT is applied to DNS traffic.	FW	NGFW-15164
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
The URL Rewrite option for Link Translation in SSL VPN Portal Service elements might not work as expected.	FW	NGFW-15386

Installation instructions

Use these high-level steps to install the SMC and the Forcepoint NGFW Engines.

For detailed information, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at https://support.forcepoint.com/Documentation.

Note: The sgadmin user is reserved for SMC use on Linux, so it must not exist before the SMC is installed for the first time.

Note: If you install the SMC on Windows 10 and Windows Defender is enabled, it might take a long time to activate a dynamic update package. For more information, see Knowledge Base article 14055.

Steps

1) Install the Management Server, the Log Servers, and optionally the Web Portal Servers.

2) Import the licenses for all components.
   You can generate licenses at https://stonesoftlicenses.forcepoint.com.

3) Configure the Firewall, IPS, or Layer 2 Firewall elements in the Management Client from the **Configuration** view.

4) To generate initial configurations, right-click each NGFW Engine, then select **Configuration** > **Save Initial Configuration**.
   Make a note of the one-time password.

5) Make the initial connection from the NGFW Engines to the Management Server, then enter the one-time password.

6) Create and upload a policy on the NGFW Engines in the Management Client.

Upgrade instructions

Take the following into consideration before upgrading licenses, 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, Knowledge Base articles, downloads, cases, and contact information.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint Next Generation Firewall Product Guide*
- Forcepoint Next Generation Firewall online Help

Note: By default, the online Help is used from the Forcepoint help server. If you want to use the online Help from a local machine (for example, an intranet server or your own computer), see Knowledge Base article 10097.

- *Forcepoint Next Generation Firewall Installation Guide*

Other available documents include:

- *Forcepoint Next Generation Firewall Hardware Guide* for your model
- *Forcepoint NGFW Security Management Center Appliance Hardware Guide*
- *Forcepoint Next Generation Firewall Quick Start Guide*
- *Forcepoint NGFW Security Management Center Appliance Quick Start Guide*
- *Forcepoint NGFW SMC API Reference Guide*
- *Stonesoft VPN Client User Guide* for Windows or Mac
- *Stonesoft VPN Client Product Guide*