



FORCEPOINT

Next Generation Firewall

Release Notes

6.5.2

Revision A

Contents

- [About this release](#) on page 2
- [Lifecycle model](#) on page 2
- [System requirements](#) on page 3
- [Build number and checksums](#) on page 6
- [Compatibility](#) on page 6
- [New features](#) on page 7
- [Enhancements](#) on page 7
- [Resolved issues](#) on page 9
- [Installation instructions](#) on page 11
- [Upgrade instructions](#) on page 12
- [Known issues](#) on page 12
- [Find product documentation](#) on page 13

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	<ul style="list-style-type: none"> • DVD drive • VGA-compatible display • Keyboard
Interfaces	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> VMware ESXi platform — <code>vmxnet3</code>. KVM platform — <code>virtio_net</code>.

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 6.5.2 is 21155.

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

- `sg_engine_6.5.2.21155_x86-64-small.iso`

```
SHA1SUM:
7e7af892bf0c0e57332f06d9d3ebe41835d0e3e4

SHA256SUM:
bc991ddf3ead7ff90fd7dde86054099de6fce105c1b4e967a9a770cb351e702f

SHA512SUM:
af26401338b0a20e1f8dba6f38cd32be
fae602feb2ac4f6f2914cb62302a6abc
f602f946c7d547ea8e52e89b8d53ab10
aa7223f89d9eabb9ff20fc368dcd1db6
```

- `sg_engine_6.5.2.21155_x86-64-small.zip`

```
SHA1SUM:
6e982522c2ce3070469b5625dd7ac2a9dad4ebe4

SHA256SUM:
ef03862a4d11d86b4beeb8f378053c145ae8f0c8e9c4cd8daa21d74142d4effe

SHA512SUM:
11a916ea33c8371f949c63f77865841e
940ae730dd04daad5a0ef44237320b45
6499008e3e8f8e41ee58640d53b859d0
33bcb4ffa904659130230a0fb459b829
```

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.

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.

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
DNS resolvers (Linux-based resolvers in particular) that rapidly issue separate queries do not work well through outbound load-balancing NAT in a Multi-Link configuration.	FW	NGFW-1645
When the same interface has an IPv4 CVI and an IPv6 CVI and NDI, but no IPv4 NDI, there might be interruptions in IPv4 traffic.	FW	NGFW-8813
When you change the Tunnel Type for a Route-Based VPN Tunnel from VPN to GRE, the change is not applied in the NGFW Engine configuration.	FW	NGFW-14175
When you add or remove an OSPFv2 Area, PIM restarts.	FW	NGFW-14397
When you remove PIM from a dynamic routing configuration that includes both OSPF and PIM, processes related to PIM might not stop correctly.	FW	NGFW-14740
When there are aggregated link interfaces in high availability mode, a cluster node in standby or offline mode might incorrectly send gratuitous ARP messages for CVIs with hardware MAC addresses when the link state or node status changes.	FW	NGFW-14834
If a TLS inspection substitute certificate for client protection expires while a session is still open, the NGFW Engine might attempt to use the expired substitute certificate instead of using the new substitute certificate.	FW, IPS, L2FW	NGFW-15262
You cannot use URL Lists for URL filtering with ports other than 80, 8080, and 443.	FW, IPS, L2FW	NGFW-15382
When connections for browser-based user authentication use HTTPS and the server certificate is signed by an external CA that has an intermediate certificate, the intermediate certificate is not presented to the client. The client does not connect due to a certificate error.	FW	NGFW-15391
If the node in a cluster that is handling a VPN connection unexpectedly loses power, outgoing VPN traffic might be interrupted for a few minutes when the connection is transferred to another node.	FW	NGFW-15519
Redirecting traffic to a Proxy Server might not work with Firewall Clusters that use load balancing if the traffic does not have dynamic source NAT applied to it.	FW	NGFW-15546
In rare cases when you use NAT for application routing on a cluster, the connection might be allowed through one node, but the reply packet might be discarded by another node.	FW	NGFW-15596
Even though ECA clients are able to communicate with the NGFW Engine, the following message might incorrectly appear in the logs: "Connection severed: CORRUPTION".	FW, IPS, L2FW	NGFW-15626
Rule counter analysis might count a connection twice when the connection has first potentially matched a rule, but then been allowed only by a later rule.	FW, IPS, L2FW	NGFW-15637
When a server included in the AD Domain is unreachable, the user identification process might temporarily stop working.	FW, IPS, L2FW	NGFW-15674
VPN monitoring might show the status "ERROR" for a tunnel with a dynamic endpoint that has a contact IP address defined.	FW	NGFW-15692

Description	Role	Issue number
When deep inspection is enabled for RTSP traffic, related connections might not be allowed.	FW, IPS, L2FW	NGFW-15704
On clusters, information about previous IPsec SAs is not correctly cleared. Keeping the information in memory increases the memory use of the VPN process.	FW	NGFW-15721
Route-Based VPN Tunnels with the VPN Tunnel Type do not enforce link selection based on QoS Class.	FW	NGFW-15745
If an NGFW Engine has the "Node-Initiated Contact to Management Server" option enabled and a backup control interface configured, communication with the Management Server is not reliable through the backup control interface.	FW, IPS, L2FW	NGFW-15747
When you use TLS inspection, clients must directly trust the CA certificate that has issued the certificate that the NGFW Engine uses to sign the substitute certificates that it generates. TLS inspection does not provide intermediate CA certificates to clients.	FW, IPS, L2FW	NGFW-15825
Category-based URL filtering might show uncategorized URLs as belonging to other categories.	FW, IPS, L2FW	NGFW-15881
When you use dynamic routing, removing a self route fails if there is a similar static route.	FW	NGFW-15934
If dynamic routing is configured in an environment with Virtual NGFW Engines, the Master NGFW Engine might restart when you install a policy on multiple Virtual NGFW Engines at the same time.	FW	NGFW-15964
When the route map that is selected as the redistribution filter in a BGP Profile element includes a community, changes to the community setting in the route map are not updated on BGP peers.	FW	NGFW-15992
A node in a cluster that is transitioning to the offline state might restart unexpectedly.	FW, IPS, L2FW	NGFW-16013
When you use DHCP relay, the NGFW Engine incorrectly uses NDI addresses to forward server responses to the client.	FW	NGFW-16124
When you change the OSPF interface type for point-to-point interfaces, the OSPF routing process might restart.	FW	NGFW-16133
If an error occurs in a Global Threat Intelligence (GTI) file reputation scan, the inspection process might restart on the NGFW Engine.	FW, IPS, L2FW	NGFW-16337
If initial contact is manually interrupted when the NGFW Engine is making initial contact for the first time, initial contact might fail. For more information and a workaround, see Knowledge Base article 16626 .	FW, IPS, L2FW	NGFW-16360
Log entries might be sent to the Log Server out of chronological order. Handling the log entries causes an increased load on the Log Server, which can cause the statuses of monitored elements to change rapidly between different status colors.	FW, IPS, L2FW	NGFW-16401
ICMPv6 packets from NGFW Engines that have NAT applied might have incorrect checksums.	FW	NGFW-16424
BGP graceful restart does not work if only IPv6 is in use.	FW	NGFW-16431
In rare cases, when a security parameter index (SPI) is deleted, the SPI is not deleted on all nodes in a cluster. In these cases, new VPN negotiations do not start even though there is traffic that should trigger new VPN negotiations.	FW	NGFW-16450

Description	Role	Issue number
The NGFW Engine might restart if connections that match an Access rule that uses the SSM DNS Proxy (UDP) service are allowed and the connections also match a NAT rule for Outbound Multi-Link.	FW	NGFW-16526
When routing information between nodes in a cluster is not synchronized correctly, routing can fail when a node or Virtual NGFW Engine becomes active.	FW	NGFW-16737
In rare cases, the VPN process might restart.	FW	NGFW-16763
A network announced by BGP might be removed from the configuration when additional announced networks are removed.	FW	NGFW-16766
Modifying the configuration fails if you add a Node Dedicated IP Address (NDI) to a tunnel interface and change the network at the same time.	FW	NGFW-16783

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*

