

# **FORCEPOINT**

## **Next Generation Firewall**

**Release Notes**

**6.5.6**

**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 13
- [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)
- 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  <b>Note:</b> RAID controllers are not supported.
Peripherals	<ul style="list-style-type: none"> <li>• DVD drive</li> <li>• VGA-compatible display</li> <li>• Keyboard</li> </ul>
Interfaces	<ul style="list-style-type: none"> <li>• One or more network interfaces for the Firewall/VPN role</li> <li>• Two or more network interfaces for the IPS in IDS configuration</li> <li>• Three or more network interfaces for inline IPS engine or Layer 2 Firewall</li> </ul> <p>For information about supported Ethernet interface types and adapters, see Knowledge Base article <a href="#">9721</a>.</p>

## 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: <ul style="list-style-type: none"><li>VMware ESXi 6.0 and 6.5</li><li>KVM (KVM is tested as shipped with Red Hat Enterprise Linux Server 7.4 and 7.5)</li><li>Microsoft Hyper-V on Windows Server 2012 or Windows Server 2016</li></ul> Firewall/VPN role only. An Intel 64-bit processor is required.
Interfaces	<ul style="list-style-type: none"><li>At least one virtual network interface for the Firewall/VPN role</li><li>Three virtual network interfaces for IPS or Layer 2 Firewall roles</li></ul> The following network interface card drivers are recommended: <ul style="list-style-type: none"><li>VMware ESXi platform — <code>vmxnet3</code>.</li><li>KVM platform — <code>virtio_net</code>.</li></ul>

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 6.5.6 is 21353.

Use checksums to make sure that files downloaded correctly.

- `sg_engine_6.5.6.21353_x86-64-small.iso`

```
SHA1SUM:
48e8a16fdfb7b8d7b625c8005cc0aa4b597df504

SHA256SUM:
7a1edd53323169ad5a84406c15f8e61f6a7f3f5632069d0c7dd21e788c348483

SHA512SUM:
70f26a3fdec202c8521242df7da2c887
6a3e43ba2f54061ce20bb4e513ce61d5
500760efee6f7b0f0499bbd4b41d6e33
4e057d629843b2fc5fd8e48a2d2cceb
```

- `sg_engine_6.5.6.21353_x86-64-small.zip`

```
SHA1SUM:
4dd36af649ba248eab98d463ae9c9e96d6b6a670

SHA256SUM:
7652bd2a125d320d8449f1c72118b6c0102f2460bdc9bf23b42a80bdac25aa4

SHA512SUM:
322a8091d13dbc5a437519140a5d7475
58ddabebe20d343c341911286f1c3be9
c7fc193b3fa0b4d98e72e8e1440c627c
e87c7029d5a89c9887677b93ac7cc53a
```

## 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 <a href="#">16290</a> .
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 <a href="#">17375</a> .

## 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
Status monitoring on the Interfaces tab of the Info pane might incorrectly show the port type as OTHER or Radio instead of the actual port type for some 40 Gbps and 10 Gbps network interfaces on NGFW appliances.	FW, IPS, L2FW	NGFW-9149
In rare cases, the NGFW Engine might temporarily send encrypted packets from the wrong interface.	FW	NGFW-13803
When the Always Keep Tunnels Established option is enabled in a VPN profile, an offline node in a cluster might initiate VPN negotiations.	FW	NGFW-17440
When many Sidewinder Proxies are configured, policy installation might take too long and traffic that is processed through the proxies might stop.	FW	NGFW-19012
When an NGFW Engine cluster starts using a new certificate for certificate-based authentication in a VPN, the certificate might not work on all nodes of the cluster.	FW	NGFW-19932
Adding a large number of blacklist entries at the same time might take longer than expected.	FW, IPS, L2FW	NGFW-20095
When using Global Threat Intelligence (GTI), you might frequently see the information message "GTI not available" in log entries.	FW, IPS, L2FW	NGFW-20155
The passive termination feature might inadvertently terminate a connection when the decision is made based on file filtering.	FW, IPS, L2FW	NGFW-20235
In a Session Initiation Protocol (SIP) control connection, the NGFW Engine does not translate the address and port information in the Via header when NAT is applied to the connection.	FW	NGFW-20346

Description	Role	Issue number
In Multi-Link VPNs, when an endpoint that has a dynamic IP address uses an IP address as the Phase-1 identity, connections might not be transferred to the VPN link when another VPN link is not available.	FW	NGFW-20860
When the NGFW Engine is upgraded locally using the sg-upgrade command, the --ignore-exp flag is not taken into account.	FW, IPS, L2FW	NGFW-20915
In SMC 6.6.2 or higher, traffic might match the wrong rule if the policy includes an Access rule in which the action options are set to forward traffic.	FW	NGFW-20968
In rare cases when you use file filtering, TLS inspection, or URL categorization, the NGFW Engine might keep connections open in the TCP Close Wait state indefinitely. As a result, the NGFW Engine might run out of memory.	FW, IPS, L2FW	NGFW-21013
Web traffic might be discarded due to Access rule conflicts. The related log entries include the following message: Connection dropped due to conflicting rule @X, initially allowed by @X.	FW, IPS, L2FW	NGFW-21563
In rare cases, the NGFW Engine might restart during policy installation if VPNs have been configured.	FW	NGFW-21862
When an NGFW Engine has more than 64 VLANs configured and you add or delete a VLAN, the change is not applied even though policy installation succeeds. Other changes to the network configuration, such as adding routes, also fail in this situation. The same issue can occur when an NGFW Engine has a large number of tunnel interfaces. Changes to the network configuration are applied only when you restart the NGFW Engine.	FW, IPS, L2FW	NGFW-21868
When node-initiated contact is configured for the NGFW Engine, if the connection to the Management Server is lost and the NGFW Engine does not receive an ICMP error message from the adjacent network device or any messages from other network devices, the NGFW Engine tries to reconnect to the Management Server only after TCP idle timeout.	FW, IPS, L2FW	NGFW-22040
When you enable the dynamic routing setting Use Equal-Cost Multi-Path (ECMP), ECMP is not enabled on BGP routes.	FW	NGFW-22049
Recordings of traffic are not saved correctly on Virtual NGFW Engines even though recording is enabled in the logging options in the inspection policy.	FW, IPS, L2FW	NGFW-22067
The inspection process might restart if traffic matches a rule that uses a Network Application as matching criteria and forwards the traffic to a Proxy Server with the Redirect Only option enabled.	FW	NGFW-22118
In rare cases, the NGFW Engine might restart if traffic matches an outbound balancing NAT rule and deep inspection is enabled.	FW	NGFW-22128
You cannot use a dynamic IPv6 address as a VPN endpoint.	FW	NGFW-22163
When you select the "Limit by" option in the Capture Traffic tool, traffic captures do not work.	FW, IPS, L2FW	NGFW-22383
The dynamic routing border gateway protocol (BGP) might not work correctly on a load balancing NGFW Engine cluster if you configure it on the NGFW Engine command line.	FW	NGFW-22385
In an environment with Multi-Link VPN tunnels that use an FQDN that resolves to both an IPv4 and IPv6 address, when you view the status of VPN tunnels in the SD-WAN dashboard, the health value for a VPN tunnel might be low and shown as red.	FW	NGFW-22504

Description	Role	Issue number
International characters in the Display Name field of a SIP message can cause SIP calls to not work.	FW, IPS, L2FW	NGFW-22677
If load-balancing is used on a clustered NGFW Engine, some connections might fail if destination NAT is applied to the connections and the translated IP addresses are also used for dynamic NAT.	FW	NGFW-22697
Connections that match a rule that uses a Service for a Sidewinder Proxy might fail if the connection is allowed by a Destination Zone match.	FW	NGFW-22762
If a monitoring probe has been configured for a route from a tunnel interface, but the tunnel interface is not included in any route-based VPN tunnel, all monitoring probes fail.	FW	NGFW-22874
When certificate authentication is used on a Master NGFW Engine cluster, information about the authentication domain and the RADIUS client is handled incorrectly. As a result, VPN tunnels that use certificate-based authentication might go down at policy installation.	FW	NGFW-22906
With a very large VPN configuration, policy installation might fail.	FW	NGFW-23033
In a Multi-Link VPN setup, traffic that has failed over to a standby NetLink might not be transferred back to the active NetLink as expected when the active NetLink becomes usable again.	FW	NGFW-23050
BGP routes with a non-default distance (eBGP) are not added to the routing table.	FW	NGFW-23054
The option Always Keep Tunnels Established might not work as expected when the NGFW Engine is the Phase-2 responder in a VPN negotiation.	FW	NGFW-23349

## 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, 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*

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

