FORCEPOINT

Next Generation Firewall

Release Notes

6.2.2

Revision A

Contents

About this release

This document contains important information about this release of Forcepoint™ Next Generation Firewall (Forcepoint NGFW); formerly known as Stonesoft® Next Generation Firewall by Forcepoint (Stonesoft NGFW).

We strongly recommend that you read the entire document.

Lifecycle model

This release of Forcepoint NGFW is a Feature Stream (FS) version.

Support for Feature Stream versions is discontinued when a new major version of Forcepoint NGFW is available.

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 Knowledge Base article 10192.

System requirements

Make sure that you meet these basic hardware and software requirements.

Forcepoint NGFW appliances

We strongly recommend using a pre-installed Forcepoint NGFW appliance as the hardware solution for new Forcepoint NGFW installations.

Note: Some features in this release are not available for all appliance models. See Knowledge Base article 9743 for up-to-date appliance-specific software compatibility information.

Two Forcepoint NGFW engine images are available:

- x86-64 — A 64-bit image that includes the Local Manager.
- x86-64-small — A 64-bit image that does not include the Local Manager.

Note: If you do not use the Local Manager, we recommend that you use the x86-64-small image. Some appliance models support only the x86-64-small image.

The following table shows whether you can use an appliance model in the Firewall/VPN (FW), IPS, or Layer 2 Firewall (L2FW) role, and the image that is supported.

Appliance model	Roles	Images
FW-315	FW	The image that does not include the Local Manager is supported
320X (MIL-320)	FW	Both images are supported
IPS-1205	IPS, L2FW	Both images are supported
FWL321	FW	The image that does not include the Local Manager is supported
NGF321	FW, IPS, L2FW	Both images are supported
FWL325	FW	The image that does not include the Local Manager is supported
NGF325	FW, IPS, L2FW	Both images are supported
110	FW	The image that does not include the Local Manager is supported
115	FW	The image that does not include the Local Manager is supported
1035	FW, IPS, L2FW	Both images are supported
1065	FW, IPS, L2FW	Both images are supported
1301	FW, IPS, L2FW	Both images are supported
1302	FW, IPS, L2FW	Both images are supported
1401	FW, IPS, L2FW	Both images are supported
1402	FW, IPS, L2FW	Both images are supported
3201	FW, IPS, L2FW	Both images are supported

Appliance model	Roles	Images
3202	FW, IPS, L2FW	Both images are supported
3205	FW, IPS, L2FW	Both images are supported
3206	FW, IPS, L2FW	Both images are supported
3207	FW, IPS, L2FW	Both images are supported
3301	FW, IPS, L2FW	Both images are supported
3305	FW, IPS, L2FW	Both images are supported
5201	FW, IPS, L2FW	Both images are supported
5205	FW, IPS, L2FW	Both images are supported
5206	FW, IPS, L2FW	Both images are supported

Sidewinder S-series appliances

These Sidewinder appliance models can be re-imaged to run Forcepoint NGFW software.

Appliance model	Roles	Images
S-1104	FW	Both images are supported
S-2008	FW	Both images are supported
S-3008	FW	Both images are supported
S-4016	FW	Both images are supported
S-5032	FW	Both images are supported
S-6032	FW	Both images are supported

Certified Intel platforms

We have certified specific Intel-based platforms for Forcepoint NGFW.

The tested platforms can be found at https://support.forcepoint.com under the Forcepoint Next Generation Firewall product.

We strongly recommend using certified hardware or a pre-installed Forcepoint NGFW appliance as the hardware solution for new Forcepoint NGFW installations. If it is not possible to use a certified platform, Forcepoint NGFW can also run on standard Intel-based hardware that fulfills the hardware requirements.

Basic hardware requirements

You can install Forcepoint NGFW on standard hardware with these basic requirements.

- (Recommended for new deployments) Intel® Xeon®-based hardware from the E5-16xx product family or higher

Note: Legacy deployments with Intel® Core™2 are supported.

- IDE hard disk and DVD drive

Note: IDE RAID controllers are not supported.

- Memory:
  - 4 GB RAM minimum for x86-64-small installation
  - 8 GB RAM minimum for x86-64 installation
- VGA-compatible display and keyboard
- 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 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.

- (Recommended for new deployments) Intel® Xeon®-based hardware from the E5-16xx product family or higher

Note: Legacy deployments with Intel® Core™2 are supported.

- One of the following hypervisors:
  - VMware ESXi 6.1 and 6.5
  - KVM (KVM is tested as shipped with Red Hat Enterprise Linux Server 7.1 and 7.2)
- 8 GB virtual disk
- 4 GB RAM minimum

- A minimum of one virtual network interface for the Firewall/VPN role, three for IPS or Layer 2 Firewall roles

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.

Build version

Forcepoint NGFW 6.2.2 build version is 18062.

Product binary checksums

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

- sg_engine_6.2.2.18062_x86-64.iso

```
SHA1SUM:
e3d481af362c5a9788a215cf4c2a60965824b25e

SHA256SUM:
3af1f3904849b0b1ff4bdc7aa7dfedc9b2c8a266ea1fcbf027311d8e88767e3d

SHA512SUM:
f49124ad6dd592d0b2253ccad96d975b
ac84a41f4f07e2f4b816cd2e394d0cdd
e329504637f0b1551ae27e0aac33d976
558b64e48dbb0871b859e6f1cd0c4daa
```

- sg_engine_6.2.2.18062_x86-64.zip

```
SHA1SUM:
cc3c508b4d32d7537726635fda816a83bd01a745

SHA256SUM:
2abccb9dcf40a6a158bd320a076b94f219b6901def15dca60e8f9a3239b26275

SHA512SUM:
9eb026defaab095753a7d940f5174d6f
2e03a9399304fef27e1c7308d4f23dbd
0e9fd5e09597e32db9ff7348507abaf1
43a7853750b7bfa84a923c500c6c3b21
```

- sg_engine_6.2.2.18062_x86-64-small.iso

```
SHA1SUM:
2f5c6a8520bfa9ecc3fcb2c304732becc0a0fe2e

SHA256SUM:
7dfc28d29c2daf216122cc6c75f2327f6ba35c27947e51c4ee5ff1c5fa956141

SHA512SUM:
92d5319b0d0247acd10e8cf1e9f0342c
884ba1f47a539e9a6c5213100609b7df
cc6aa3b4f74b93836dae2af7b5c2970b
a4a0a3bdacf75ee1daf043f080f815d5
```

- sg_engine_6.2.2.18062_x86-64-small.zip

```
SHA1SUM:
729484c56dea478769494e5d438683221b403f4a

SHA256SUM:
bacc1396c12f8473aa96310e3868da937f44d2f3407a9ca62dc98d9335afd05d

SHA512SUM:
3ac59f098bf19bb69771cb378ff18275
154cd2978cfcce472a9b24973192cc7a
9ef7752f02ec84ce8afbdd99298dd07e
e15d0995ec10ac84bc5377ce96d5619d
```

Compatibility

Forcepoint NGFW 6.2 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.2 or later
- Dynamic Update 864 or later
- Stonesoft® VPN Client for Windows 6.0.0 or later
- Stonesoft® VPN Client for Mac OS X 2.0.0 or later
- Stonesoft® VPN Client for Android 2.0.0 or later
- Server Pool Monitoring Agent 4.0.0 or later
- McAfee® Logon Collector 2.2 and 3.0
- McAfee® Advanced Threat Defense 3.6
- McAfee Endpoint Intelligence Agent (McAfee EIA) 2.5

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*.

Forcepoint Advanced Malware Detection

Forcepoint Advanced Malware Detection uses file reputation scans in a sandbox service to detect advanced threats. The Cloud Sandbox analyzes the behavior of files in a restricted operating system environment and returns a reputation score for the files. From the Logs view of the Management Client, you can access an external portal where you can view detailed reports for files that have been analyzed in the Cloud Sandbox. You can also use analysis and reporting tools in the external portal.

Note: Forcepoint Advanced Malware Detection requires a separate license for the Cloud Sandbox service. See Knowledge Base article 12514.

Pending configuration changes shown for NGFW Engines

You can now view configuration changes that you and other administrators have made before the new configurations are transferred to the engines. The pending changes are shown in the Home view and on the selected engine's home page. You can optionally also enforce an approval workflow. When an approval workflow is enforced, administrators with unrestricted permissions must approve all pending changes before the changes can be committed.

Support for Sidewinder Proxies on Virtual NGFW Engines in the Firewall/VPN role

You can now use Sidewinder Proxies (HTTP, SSH, TCP, and UDP) on Virtual NGFW Engines in the Firewall/VPN role. Sidewinder Proxies on Forcepoint NGFW enforce protocol validation and restrict the allowed parameters for each protocol. Sidewinder Proxies are primarily intended for users in high assurance environments, such as government or financial institutions. In environments that limit access to external networks or access between networks with different security requirements, you can use Sidewinder Proxies for data loss protection.

DNS Relay on NGFW Engines in Firewall/VPN role

DNS relay allows NGFW Engines in the Firewall/VPN role to provide DNS services for internal networks. The firewall forwards DNS requests from clients in the internal network to remote DNS servers and temporarily stores the results of the DNS requests in the cache. The firewall can forward DNS requests to different DNS servers depending on the domain in the DNS request. The firewall can also return fixed DNS results for specific hosts or domains, and translate external IP addresses in DNS replies to IP addresses in the internal network.

Improved dynamic multicast routing support on NGFW Engines in Firewall/VPN role

You can now configure protocol-independent multicast (PIM) on NGFW Engines in the Firewall/VPN role in the Management Client. Previously, you could only configure PIM on the engine command line. You can use source-specific multicast (PIM-SSM), sparse mode (PIM-SM), or dense mode (PIM-DM).

Improved logging and diagnostics for SSL VPN Portal

Logging and diagnostics have been improved for the SSL VPN Portal. Log entries are generated when an SSL VPN Portal user starts and ends a session. If diagnostics are enabled for the SSL VPN Portal, log entries are also generated for HTTP or HTTPS transactions. SSL VPN Portal users can see the time of their last logon and the number of failed logon attempts in the status bar of the SSL VPN Portal.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 6.2.0

Enhancement	Description
NetLink-specific DNS IP addresses	You can now define NetLink-specific DNS IP addresses for static NetLinks. Dynamic NetLinks can automatically learn DNS IP addresses.
Improved configuration of User Responses	User Responses are now easier to configure. The new message response allows you to quickly create simple messages without using HTML markup. You can also use variables in User Responses to provide connection-specific information to the end users.

Enhancements in Forcepoint NGFW version 6.2.1

Enhancement	Description
Improved scaling of dynamic routing for Virtual NGFW Engines	Dynamic routing now scales up better with a large number of Virtual NGFW Engines.
Cloud Sandbox logging has been enhanced	A file allowed through an NGFW Engine and later found to be malicious previously created only a "File reputation updated" log entry. Now also a log entry with the "File_Malware-Detected" Situation is displayed. Logs did not previously indicate that unsupported file types were sent to the Cloud Sandbox for inspection. Now "Sandbox_Unsupported-File-Type" Situations are logged when an unsupported file type has been sent to the Cloud Sandbox.

Enhancements in Forcepoint NGFW version 6.2.2

Enhancement	Description
Log rate and spooled log information available in engine status monitoring	In the engine status monitoring, you can now see the log rate and the times at which logs have been spooled on the engine.
Improved dynamic routing monitoring	Changes in the OSPF and BGP neighborhood trigger alerts that are visible in the Logs view of the Management Client. Information about route changes is also included in logs.
Improved inspection for flash files	The NGFW Engine now supports the inspection of flash files, allowing it to detect potential security threats in flash files.
Faster rule matching for dynamic elements	Rule matching for rules that contain DNS names, users, and user groups is now faster. This improvement is especially useful when the policy uses a large number of these elements.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in earlier releases, see the Release Notes for the specific release.

Description	Role	Issue number
The tcpdump utility that is included in the NGFW Engine software has been updated to version 4.9.2 to address multiple potential security and denial of service issues.	FW, IPS, L2FW	NGFW-2998
After the certificate for an engine node has been renewed, the engine might continue to use a backup of the previous certificate instead of the new certificate. This issue can happen after automatic certificate authority (CA) renewal, when the type of CA changes, or after automatic node certificate renewal.	FW, IPS, L2FW	NGFW-3178
When you use the cloud sandbox for Forcepoint Advanced Malware Detection, memory consumption can increase significantly.	FW, IPS, L2FW	NGFW-4468
When you use McAfee GTI, memory consumption might increase significantly and cause the NGFW Engine to become unstable.	FW, IPS, L2FW	NGFW-4554
If deep inspection records the matching traffic, some CPUs can be fully utilized, which causes traffic to be processed slowly for some connections.	FW, IPS, L2FW	NGFW-4637
When the SSM HTTP Proxy processes certain types of HTTP traffic, the proxy process might restart.	FW	NGFW-4942
If you configure protocol-independent multicast (PIM) routing using the Management Client, then change the PIM configuration on the command line using VTYSH, the PIM configuration files might be overwritten.	FW	NGFW-5110
If you disable a node in a cluster, but do not remove it from the network, when you refresh the policy in the other nodes in the cluster, there can be issues with state synchronization until the NGFW Engines are restarted. You should only disable a node when a cluster member has failed and hardware needs to be replaced. A cluster member that is present in the network must not be disabled.	FW, IPS, L2FW	NGFW-5229
When VPN tunnels are negotiated with a large number of different endpoints, the memory consumption in the NGFW Engine might increase substantially.	FW	NGFW-5251
If the "Log URL Categories" option is set to "Enforced" in the logging options, TLS connections might not be decrypted even if TLS decryption is enabled for the NGFW Engine.	FW, IPS, L2FW	NGFW-5282
If the NGFW Engine is processing both IPv4 and IPv6 traffic, some related connections might not get through.	FW, IPS, L2FW	NGFW-5435
If the rule that allows FTP connections matches Network Applications or logs information about application detection, but does not have deep inspection or file filtering enabled, related connections for FTP might not be allowed.	FW, IPS, L2FW	NGFW-5477
When file filtering blocks a file, and a user response is configured for the connection, some CPUs can be fully utilized, which causes traffic to be processed slowly for some connections.	FW, IPS, L2FW	NGFW-5705

Description	Role	Issue number
If a VPN configuration is large and refreshing the policy causes a large number of tunnels to be reconfigured, the refreshing of the policy can time out.	FW	NGFW-5708
The NGFW Engine might be unstable with newer CPU models due to incompatible features that have been enabled.	FW, IPS, L2FW	NGFW-5844
In rare cases, the inspection process or the NGFW Engine might restart when file filtering or deep inspection is applied to traffic.	FW, IPS, L2FW	NGFW-5861
When the engine inspects specific tunneled traffic, the engine might restart in the following cases: • A rule in the Inspection Policy uses the "Terminate: Passive and Silent" action to log that termination could have occurred, but does not stop the traffic. • The value of the "Action if Limit Exceeded" option for "Limit for Rematching Tunneled Traffic" is "Allow".	IPS, L2FW	NGFW-5865
When the Tunnel Type is "VPN" for a tunnel in the route-based VPN and you use OSPF dynamic routing with the tunnel, routing information received from a neighbor might not be accepted.	FW	NGFW-5899
When a Virtual NGFW Engine is moved to a different Master NGFW Engine node, IPv6 routes might not be propagated from BGP to the routing table for the Virtual NGFW Engine. Routes might be visible when you use VTYSH, but they do not appear in the Virtual NGFW Engine.	FW	NGFW-5901
When you use a Virtual Firewall as a VPN endpoint and you use certificates for authentication, VPN negotiation might fail if there are too many simultaneous VPN tunnel negotiations.	FW	NGFW-5904
When you use loose connection tracking mode and connections are closed in a specific way, the connections are not removed from the engine's connection table until the idle timeout limit is reached. The existing connection prevents new connections from being established with the same source and destination IP addresses and ports until the existing connection is removed from the connection table.	FW, IPS, L2FW	NGFW-6046
When dynamic routing fails over, synchronized forwarding information base (FIB) routes might not be removed correctly.	FW	NGFW-6193
If you do not use an HTTP proxy to connect to the ThreatSeeker Intelligence Cloud server, URL filtering status is not shown on the status card for the NGFW Engine.	FW, IPS, L2FW	NGFW-6210
When you remove an automatic blacklist entry that was created by an engine from the Blacklist view, the command fails. The following message is shown: "Command failed (113)".	FW, IPS, L2FW	NGFW-6265
If Access rules use the FTP Protocol Agent and deep inspection is not enabled, the NGFW Engine might restart when you install the policy after adding or removing an interface.	FW	NGFW-6500
When you use a fully qualified domain name (FQDN) as the contact address for a VPN endpoint, and the DNS resolution changes, VPN connections stop working.	FW	NGFW-6602

Description	Role	Issue number
If a Virtual Firewall is used as a VPN gateway, and the Virtual Firewall is moved to a different Master NGFW Engine node, VPN traffic might be disrupted until the VPN tunnels are renegotiated.	FW	NGFW-6607
Certain types of TCP keep-alive packets might be dropped if deep inspection is enabled.	FW, IPS, L2FW	NGFW-6858
Access rules that match based on the source VPN might match non-VPN traffic if the source, destination, and service match the connection, and deep inspection, application matching, or application logging is enabled.	FW	NGFW-7092
Logs of the type Connection_Allowed do not show the destination interface, destination VLAN, or destination zone if the connection that generated the log entry was inspected.	FW, IPS, L2FW	NGFW-7142
If SNMP is configured, it does not work with interfaces that have PPP enabled.	FW	NGFW-7223
When the NGFW Engine processes a large number of SIP connections and NAT is used, the inspection process might restart.	FW	NGFW-7270
When a concurrent connection limit is configured and set to Refuse in the action options of an Access rule, the NGFW Engine might become unresponsive until you restart the NGFW Engine.	FW, IPS, L2FW	NGFW-7311
If IPv6 addresses have been configured for a Virtual NGFW Engine, the Master NGFW Engine might restart when the policy is installed or refreshed.	FW	NGFW-7340
The redirection link on the logon page for browser-based user authentication does not work if the URI includes a port.	FW	NGFW-7641
VPN negotiation might fail if a VPN endpoint in a Multi-Link VPN has a dynamic IP address and a static contact address.	FW	NGFW-7649
Browser-based user authentication might not work correctly when dynamic routing is configured for the same NGFW Engine. This issue prevents the policy from being successfully refreshed on the NGFW Engine, and prevents the use of browser-based user authentication.	FW	NGFW-7746
When McAfee Endpoint Intelligence Agent is integrated with NGFW, memory consumption on the NGFW Engine can increase significantly.	FW, IPS, L2FW	NGFW-7819

Installation instructions

Use these high-level steps to install 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.

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

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 with the Management Client using the **Configuration** view.

4) To generate initial configurations for the engines, right-click each Firewall, IPS, or Layer 2 Firewall element, then select **Configuration** > **Save Initial Configuration**.
   Make a note of the one-time password.

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

6) Create and upload a policy on the engines using the Management Client.

Upgrade instructions

Take the following into consideration before upgrading licenses, engines, and clusters.

- Upgrading to version 6.2 is only supported from version 5.10 or later. If you have an earlier version, first upgrade to version 5.10.
- Forcepoint NGFW version 6.2 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 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*.
- Changes to category-based URL filtering in Forcepoint NGFW version 6.1 affect all existing users of category-based URL filtering. Legacy URL Situation elements can no longer be used in policies for Forcepoint NGFW version 6.1 or later. If rules in your policy contain legacy URL Situation elements, you must replace them with URL Category elements. See the *Forcepoint Next Generation Firewall Product Guide* for detailed instructions.
- Starting from Forcepoint NGFW version 6.2, the Anti-Spam feature is no longer supported. See Knowledge Base article 12394. If you require this feature, we recommend that you use the most recent Long-Term Support (LTS) version. See Knowledge Base article 10192. If you require a comprehensive Anti-Spam and Email Security solution, we recommend that you use Forcepoint Email Security Cloud.
- The way that routes defined in the Management Client are handled by Quagga has changed. In Forcepoint NGFW version 6.0 and earlier, static routes that you defined in the Management Client were considered kernel routes in Quagga. When redistributing these to dynamic routing protocols, you could use the "redistribute kernel" command.
  Starting from Forcepoint NGFW version 6.1.0, static routes that you define in the Management Client are considered static routes in Quagga. This change affects, for example, redistributing routes that you define in the Management Client to the dynamic routing protocols. Configuring static routes using vtysh in Quagga is no longer supported. Use the Management Client to configure static routing.

Known issues

For a list of known issues in this product release, see Knowledge Base article 12476.

Known limitations

This release of the product includes these known limitations.

Limitation	Description
Inspection in asymmetrically routed networks	In asymmetrically routed networks, using the stream-modifying features (TLS Inspection, URL filtering, and file filtering) can make connections stall.
Inline Interface disconnect mode in the IPS role	The *disconnect mode* for Inline Interfaces is not supported on IPS virtual appliances, IPS software installations, IPS appliance models other than IPS-6xxx, or modular appliance models that have bypass interface 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*