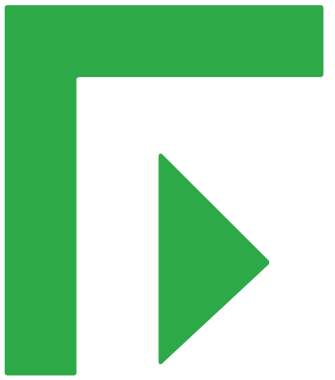

FORCEPOINT

Stonesoft Next Generation Firewall

Release Notes

6.1.1

Revision A

Table of contents

About this release

This document contains important information about this release of Stonesoft® Next Generation Firewall by Forcepoint (Stonesoft NGFW; formerly known as McAfee® Next Generation Firewall). We strongly recommend that you read the entire document.

Lifecycle model

This release of Stonesoft Next Generation Firewall is a Feature Stream (FS) version.

Support for Feature Stream versions is discontinued when a new major version of Stonesoft Next Generation Firewall 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 Stonesoft Next Generation Firewall lifecycle policy, see Knowledge Base article 10192.

System requirements

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

Stonesoft NGFW appliances

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

Appliance model	Roles	Images
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
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 Stonesoft 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 Stonesoft NGFW.

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

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

Basic hardware requirements

You can install Stonesoft 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 CD 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 Engine requirements

Master Engines have specific hardware requirements.

- Each Master Engine must run on a separate physical device. For more details, see the *Stonesoft Next Generation Firewall Installation Guide*.
- All Virtual Security Engines hosted by a Master Engine or Master Engine cluster must have the same role and the same Failure Mode (*fail-open* or *fail-close*).
- Master Engines can allocate VLANs or interfaces to Virtual Security 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 Engine cluster in standby mode.
- Cabling requirements for Master 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 *Stonesoft Next Generation Firewall Installation Guide*.

Virtual appliance node requirements

You can install Stonesoft 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 5.5 and 6.0
  - 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 Stonesoft 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 Stonesoft NGFW is run as a virtual appliance node in the IPS or Layer 2 Firewall role, clustering is not supported.

Build version

Stonesoft Next Generation Firewall 6.1.1 build version is 17035.

Product binary checksums

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

- sg_engine_6.1.1.17035_x86-64.iso

```
SHA1SUM:
59b3464926c09488847512aa3f3adac487a729e0

SHA256SUM:
29be8914eac233a355fc0323fe197cdef08f54be3f016b8a3dfe52d5e00309b0

SHA512SUM:
2f6fea55bd294b869001b363ee9028fd
343a36bd75400a1fa5b861faf9ec61f0
71a27a64742320cd1713bfdbe6c4714a
0855b1e8223a4b360e4561a8a67ecfb3
```

- sg_engine_6.1.1.17035_x86-64.zip

```
SHA1SUM:
622032217e77cb2e0cfeb67d9ded2d0110f6fa62

SHA256SUM:
c4fc4e2f897b46d1c79259dc6b636aac6d67ef0aa5ced1a15d5ad199758faf2a

SHA512SUM:
c8378657ca77e606de263761374c6795
36a06e844201c6b835784061711ddd11
40071a7039ac1f73f54ce44eed82c285
2996b13951c4b282e74f9caa204fe479
```

- sg_engine_6.1.1.17035_x86-64-small.iso

```
SHA1SUM:
e0e450676727fb8ffd586999de898b49803572a3

SHA256SUM:
61cd56a7ffb98a7a2225b2204850bd840aa99b5a0e57290c5815a66a941afd69

SHA512SUM:
ffb0feac4c7dbcb8260af3be602e4efe
b764902c63b1163e5e068ef43982e14c
5373aa5fa4a87ecc9bed14d141674a51
e2dfc563761e15f3a04dfaa1c52100d6
```

- sg_engine_6.1.1.17035_x86-64-small.zip

```
SHA1SUM:
12869a57c3ffdf050991318e2a9bfd9c2b36140c

SHA256SUM:
549f171df9dc123d2c0c90500ba802eaa85784f2f5b5ec2c31a277291ecfd5e4

SHA512SUM:
798daf7d2e91f3ef3a935351567667ba
6423d127f64aabb282a230f958160805
e222aa8fbf7c0a6cddc16b439359fb27
23ae675584a539de848ee4ba25265c5f
```

Compatibility

Stonesoft NGFW 6.1 is compatible with the following component versions.

- Stonesoft® Management Center (SMC) 6.1 or later
- Dynamic Update 810 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 *Stonesoft Next Generation Firewall Product Guide* and the *Stonesoft Next Generation Firewall Installation Guide*.

Geo-protection and IP address categorization

You can now configure geo-protection to allow or block traffic. There are predefined Country elements that represent IP addresses registered in specific countries. You can use Country elements to filter traffic in Access rules based on the source or destination country, or entire continents. They can also be used in NAT rules, Inspection rules, and File Filtering rules.

You can use predefined IP address lists to control access to known good or bad IP addresses. You can either use the predefined IP address lists or create new IP address lists. You can also import IP address lists through the SMC API to the SMC. For more information, see the *Stonesoft SMC API Reference Guide*.

Integration of Sidewinder Proxies

On Sidewinder firewalls, proxies provide high assurance protocol validation. On Stonesoft NGFW, Sidewinder Proxies enable some of the proxy features that are available on Sidewinder. In Stonesoft NGFW version 6.1, the following Sidewinder Proxies are supported: HTTP, SSH, TCP, and UDP.

You can use Sidewinder Proxies on Stonesoft NGFW to enforce protocol validation and to 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.

Changes in category-based URL filtering

Category-based web filtering now uses URL categories provided by Forcepoint™ ThreatSeeker® Intelligence Cloud. There are new types of elements for configuring URL filtering:

- URL Category elements are Network Application elements that represent the categories for category-based URL filtering.
- URL Category Group elements contain several related URL Categories.
- URL List elements are Network Application elements that allow you to manually define lists of URLs that you want to allow or block.

The way that category-based URL filtering is applied to traffic has changed. You can now use URL Categories, URL Category Groups, and URL Lists in the Service cell of Access rules to configure URL filtering. It is no longer possible to configure URL filtering using Situation elements in the Inspection Policy.

Note: These changes affect all existing users of category-based URL filtering. Legacy URL Situation elements can no longer be used in policies for Stonesoft NGFW version 6.1 or higher. If rules in your policy contain legacy URL Situation elements, you must replace them with URL Category elements.

Browser-based wizard for configuring NGFW appliances

As an alternative to using the command-line version of the NGFW Initial Configuration Wizard (sg-reconfigure) to configure an NGFW appliance, you can now use an initial configuration wizard in a web browser.

Redirection of web traffic to TRITON AP-WEB Cloud

TRITON® AP-WEB Cloud is a cloud-based web security proxy service. Stonesoft NGFW can now redirect web traffic to the TRITON® AP-WEB Cloud for inspection. Stonesoft NGFW redirects web traffic to the TRITON

AP-WEB Cloud using a predefined policy-based VPN. The traffic is inspected in the TRITON AP-WEB Cloud and transparently forwarded to the destination.

Note: To use TRITON AP-WEB Cloud to inspect web traffic, you must have a subscription to the TRITON AP-WEB Cloud service.

In addition to an IPv4 or IPv6 address, you can now use a fully qualified domain name (FQDN) as a dynamic contact address of an external VPN gateway. Connecting through a VPN to a dynamic FQDN endpoint allows TRITON AP-WEB Cloud to offer addresses from the geographically closest service point.

The TRITON AP-WEB Cloud service requires the endpoint to use a MAC address as a unique identifier. You can now define VPN-specific exceptions to the IKE Phase-1 ID for endpoints on VPN Gateways. Exceptions are useful in cases where an external VPN gateway requires specific information in the IKE phase-1 value.

For more information and configuration instructions, see Knowledge Base article 10582.

Enhancements

This release of the product includes these enhancements.

Enhancements in Stonesoft NGFW version 6.1.0

Enhancement	Description
Simplified service configuration and customization improvements in SSL VPN Portal	You can now allow access to intranet services in the SSL VPN Portal with a freeform URL. It is no longer necessary to configure each SSL VPN Portal service separately. End users can access the services by typing the URL directly in the SSL VPN Portal. You can now also modify the look-and-feel of the SSL VPN Portal and create a custom theme with company colors and logos for the SSL VPN Portal in the Management Client.
Fully qualified domain names as contact addresses in external VPN gateways	In addition to an IPv4 or IPv6 address, you can now use a fully qualified domain name (FQDN) as a dynamic contact address of an external VPN gateway.
VPN-specific exceptions for IKE Phase-1 ID	You can now define VPN-specific exceptions to the IKE Phase-1 ID for endpoints on VPN Gateways. Exceptions are useful in cases where an external VPN gateway requires specific information in the IKE phase-1 value.
Improved throughput for anti-malware inspection	The throughput of anti-malware inspection has been significantly improved.
Improved scaling of inspection for Virtual Security Engines	Inspection now scales up better with multiple Virtual Security Engines.
Improved TCP handling in the inspection module	TCP protocol handling in the inspection module has been enhanced for performance and compatibility.
Support for Tunnel Interfaces and unnumbered interfaces for OSPF	Support for Tunnel Interfaces and unnumbered interfaces for OSPF has been added.
Enhanced botnet detection	Botnet detection has been enhanced.
SSH server key fingerprints shown on engine console when the engine starts up	If SSH is enabled, SSH server key fingerprints are shown on the local console when the NGFW engine starts up.

Enhancements in Stonesoft NGFW version 6.1.1

Enhancement	Description
Improved logging for File Filtering	Logging for File Filtering has been improved significantly. For example, all File Filtering Situations are now logged under File Filtering in the Facility column of the Logs view.
Improved evasion detection for HTTP traffic	Deep inspection is now better able to detect evasions in HTTP traffic.
Optimized policy refresh for Virtual Security Engines	Refreshing a policy that includes inspection for a large number of Virtual Security Engines is now faster.

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
In log entries for connections that are detected on Capture Interfaces, the Physical Interface information might be incorrect.	IPS	135657
SYN flood protection might consume too much memory.	FW, IPS, L2FW	NGFW-275
When you use URL Lists in rules, the expected behavior is that URLs that contain a path do not match the rule if HTTPS traffic is not decrypted. Even when HTTPS traffic is decrypted, URLs that contain a path do not match rules that allow traffic.	FW, IPS, L2FW	NGFW-383
When the Log Server to which the engine sends log data changes, the engine might send the same alert twice. For more information, see Knowledge Base article 10541.	FW, IPS, L2FW	NGFW-469
The Protocol cell is ignored when matching connections against the Exceptions rules in the Inspection Policy. As a result, connections might match rules where the protocol identified for the connection is different from the protocol specified in the rule.	FW, IPS, L2FW	NGFW-523
On interfaces that do not have IP addresses, OSPF graceful restart might fail.	FW	NGFW-638
When the Log Accounting Information option is selected in rules for category-based URL filtering and connections that are not decrypted match the rules, the accounting information does not contain the URL Category, SNI information, or the traffic volume.	FW, IPS, L2FW	NGFW-730
Using a license that allows the use of a single CPU with hardware that has multiple CPUs causes instability.	FW, IPS, L2FW	NGFW-743
When the engine does a BGP or OSPF graceful restart, traffic might be interrupted for a few hundred milliseconds.	FW	NGFW-746
Enabling ThreatSeeker in the Engine Editor and selecting "Log URL Categories" in the Logging options of Access rules does not enable the logging of URL Categories. To log URL Categories, you must select "Log Network Applications" in the Logging options or add URL Category elements to the Service cell of Access rules.	FW, IPS, L2FW	NGFW-750
Values for some log fields are incorrectly logged twice when traffic matches URL-related Situations. The "URL", "HTTP request host", and "HTTP request method" log fields might show the text "2 values" instead of the correct value for the log field.	FW, IPS, L2FW	NGFW-763
When you inspect FTP connections, FTP file transfers might not complete successfully.	FW, IPS, L2FW	NGFW-789
If a policy contains a large number of SSM Proxy Services, or if the engine has a large number of CPU cores, the first policy installation might take a long time. Policy installation might time out.	FW	NGFW-867
The inspection process might consume too much memory when inspection is applied to HTTPS traffic, regardless of whether the HTTPS traffic is decrypted. The engine might stop processing traffic.	FW, IPS, L2FW	NGFW-941

Description	Role	Issue number
When ATD File Reputation Scan is enabled in the File Filtering Policy and configured to discard files with an unknown reputation, files might be incorrectly discarded if a response is received from the ATD server in 4 seconds or less.	FW, IPS, L2FW	NGFW-962
For some file transfers, the engine might incorrectly show "Not Available" in the ATD Reputation field of logs even though the engine receives the results of the file reputation scan from the ATD server.	FW, IPS, L2FW	NGFW-965
When you downgrade Master Engines to an earlier version of the Stonesoft NGFW engine software, the Master Engines might lose connectivity to the Management Server.	FW, IPS, L2FW	NGFW-983
If the engine does not trust the server certificate that is used to authenticate HTTPS connections and the session is resumed, the identification of detected applications and URL categories might be inconsistent.	FW, IPS, L2FW	NGFW-1046
Traffic that uses the SSM HTTP Proxy might stop.	FW	NGFW-1061
If the inspection process restarts due to a software issue, or if you manually restart the process, some or all inspected connections might be interrupted until you reboot the engine.	FW, IPS, L2FW	NGFW-1094
If you change the MTU for a Master Engine Physical Interface that has VLAN Interfaces for hosted Virtual Security Engines, the change is applied only when you reboot the Master Engine.	FW, IPS, L2FW	NGFW-1138
DHCP relay might stop working when you modify a VLAN Interface that has DHCP Relay enabled.	FW	NGFW-1274
When a large number of Virtual Security Engines use dynamic routing, refreshing the policy on the Virtual Security Engines might fail.	FW	NGFW-1276
If the user that is being authenticated belongs to a User Group that contains a large number of users, user authentication might be slow or might not work.	FW	NGFW-1279
TCP connections to the engine itself might be slow when the connection goes through an interface that uses the MOD-EM2-10G-SFP-4/MOE10F4 or MOD-40G-2/MO40F2 interface modules.	FW, IPS, L2FW	NGFW-1305
Inspection of HTTP or HTTPS traffic might stop working.	FW, IPS, L2FW	NGFW-1309
QoS cannot be applied to multicast traffic.	FW, IPS, L2FW	NGFW-1361
When you delete VPN SAs manually from a cluster in a load-balancing mode, notifications might not be sent to the VPN peers. The lack of notifications might cause small delays in the renegotiation of the VPN SAs.	FW	NGFW-1420
Forwarding VPN Client traffic from an SSL VPN tunnel to a Route-Based VPN tunnel that has the VPN tunnel type might not work correctly.	FW	NGFW-1601
Refreshing the policy on Master Engines or Virtual Security Engines might cause latency in VPN traffic.	FW, IPS, L2FW	NGFW-1616
When the SNMP agent must process a large number of ARP cache entries, SNMP queries to retrieve ARP cache entries might time out.	FW, IPS, L2FW	NGFW-1775
ICMP connections might not be cleared from the Connection Monitoring view.	FW, IPS, L2FW	NGFW-1784
When interfaces that support 10Gb or 40 Gb throughput do not have VLAN Interfaces or Aggregated Link Interfaces configured, some part of the traffic might stop flowing through the interfaces over time.	FW	NGFW-1817

Description	Role	Issue number
You cannot disable OSPF dynamic routing for Tunnel Interfaces that do not have IP addresses using the Management Client.	FW	NGFW-1900
On Firewall Clusters, the maximum throughput for some VPN connections might be lower than for other VPN connections that use the same VPN gateways.	FW	NGFW-2032
When you use a Virtual Firewall as a VPN gateway, VPN tunnels that use IKEv1 might experience intermittent issues. During the issue, the following message is shown in the logs: "IPsec SA install failed: Lost concurrent negotiation arbitration".	FW	NGFW-2082
When a remote gateway in a Multi-Link VPN has endpoints with dynamic IP addresses, policy installation might fail. The following type of error message is shown: "Engine error: Message code 208 (errno 104)Proposal <number> referring to an unsupported hash algorithm <hash>".	FW	NGFW-2084
The engine might not be able to decrypt HTTPS traffic from Google applications on Android devices.	FW, IPS, L2FW	NGFW-2116
Wireless interfaces on Stonesoft NGFW 115 appliances might experience intermittent issues.	FW	NGFW-2303

Installation instructions

Use these high-level steps to install SMC and the Stonesoft NGFW engines.

For detailed information, see the *Stonesoft 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.

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.

Note: Changes to category-based URL filtering in Stonesoft 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 Stonesoft NGFW version 6.1 or higher. If rules in your policy contain legacy URL Situation elements, you must replace them with URL Category elements. See the *Stonesoft Next Generation Firewall Product Guide* for detailed instructions.

- Upgrading to version 6.1 is only supported from version 5.10 or later. If you have an earlier version, first upgrade to version 5.10.
- Stonesoft NGFW version 6.1 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 CD and follow the instructions. For detailed instructions, see the *Stonesoft Next Generation Firewall Installation Guide*.

Known issues

For a list of known issues in this product release, see Knowledge Base article 10571.

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 *Stonesoft 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.

- *Stonesoft Next Generation Firewall Product Guide*
- Stonesoft 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.

- *Stonesoft Next Generation Firewall Installation Guide*

Other available documents include:

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

The following document included in appliance deliveries still uses the old product name and brand:

- *McAfee Security Management Center Appliance Quick Start Guide*