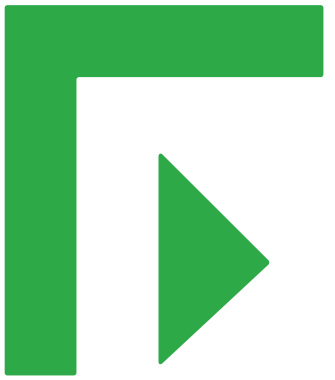

FORCEPOINT

Stonesoft Next Generation Firewall

Release Notes

5.10.9

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.

NGFW version 5.10.1 has been evaluated against the Common Criteria Network Devices Protection Profile with Extended Package Stateful Traffic Filter Firewall. For more details, see https://www.niap-ccevs.org/Product/Compliant.cfm?pid=10669.

Note: We have started rebranding the NGFW product and the NGFW product documentation. We use Stonesoft as the product name in this document. However, the old product name is still used in the NGFW appliances and the product documentation set that we created for the NGFW 5.10.0 release.

Lifecycle model

This release of Stonesoft Next Generation Firewall 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 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
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
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

    Note: Stonesoft Next Generation Firewall 5.10.9 does not support integration with Intel Security Controller and deployment on VMware NSX.

  - KVM (KVM is tested as shipped with Red Hat Enterprise Linux Server 7.0)
  - Oracle VM server 3.3 (tested with Oracle VM server 3.3.1)
- 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 5.10.9 build version is 14107.

Product binary checksums

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

- sg_engine_5.10.9.14107_x86-64.iso

```
SHA1SUM:
64fb5c66d38f4934a52d716e886e43b9a812e353

SHA256SUM:
96e8ae366e7dde6e10dfcf04c50c71c4cfb27857d2dcffa6ce39ba13dcc7b306

SHA512SUM:
fb0197f0e6e85855d503e4e36749a483
e32ff4293c66bbbdbadd0237e83a4fe9
25d2eea2292cf2541848bd7e94a84548
1f0edca999e49f93f34763371e189381
```

- sg_engine_5.10.9.14107_x86-64.zip

```
SHA1SUM:
12f92ae968e983585492c24f74a25769a80acb9c

SHA256SUM:
2d2d83cc4e7df9fca36759b16f090a135495f29f0ebf54758bde7ceaf15ce89b

SHA512SUM:
084fe58e93737ca959274fc80847870e
f373981b2f1034cd7105b9b54272c8fb
97cf4cc89b8021977531b1b61f6d21c6
ade49546806b7b95fcdd629c8e3c3a2f
```

- sg_engine_5.10.9.14107_x86-64-small.iso

```
SHA1SUM:
180b92ea8652f6d9e60f5bd0ffdb60e67ed62599

SHA256SUM:
993e37039596455738d61c2089a959cfa41c4f8fed4f21903cacac5d98a57cd1

SHA512SUM:
e6273dadc275aee638929057de9b4632
611874b8956de3bad64738bf289ed131
82228d8e6c8364a021a3746bb4810a10
c01845d5e83a2e43792ecd099c125ce9
```

- sg_engine_5.10.9.14107_x86-64-small.zip

```
SHA1SUM:
73713a3120c4c0928de8a4d631f48cff7d390bc4

SHA256SUM:
df5d7ea4482821df8dd02b8e8112a0dc704f94aa4be704aeb6917cb97a6e9fab

SHA512SUM:
3efa269514ddabc9d62d774fa196e5c7
5114da12ce16b4cc2195847342e84c74
98043f05d3cb8d15c9afed006be55a85
099c7b8932368b1601d2298b09f8f2e8
```

Compatibility

Stonesoft NGFW 5.10.9 is compatible with the following component versions.

- McAfee® Security Management Center (SMC) 5.10.0 or later
- Dynamic Update 810 or later
- Stonesoft IPsec VPN Client 5.3.0 or later
- McAfee® VPN Client for Windows 5.9.0 or later
- McAfee® VPN Client for Mac OS X 1.0.0 or later
- McAfee® VPN Client for Android 1.0.1 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*.

Note: Stonesoft Next Generation Firewall 5.10.9 does not support integration with Intel Security Controller and deployment on VMware NSX.

Support for Threat Intelligence Exchange

Stonesoft NGFW can now query file reputations and receive reputation updates from the McAfee® Threat Intelligence Exchange (TIE) server. TIE makes it possible for administrators to tailor comprehensive local threat intelligence from global intelligence data sources, such as McAfee® Global Threat Intelligence™ (McAfee GTI), endpoints, gateways, and other security components. File reputation data is exchanged using the McAfee® Data Exchange Layer (DXL) broker network. File reputation updates ensure that Stonesoft NGFW engines always have the latest file reputations available for use in file filtering.

Single sign-on (SSO) to SSL VPN Portal

The SSL VPN Portal (reverse web proxy) can be configured to cache user credentials. The portal logs on to the back-end servers with the credentials as if they came from the web browser at the endpoint. You can group the servers that use the same credentials by SSO domain, to further reduce the need to re-enter the password.

New tunnel type for the route-based VPN

A new tunnel type for the route-based VPN allows the use of tunnel mode IPsec without an additional tunneling layer. The route-based VPN configuration dialog box has been improved.

Connectivity between Stonesoft NGFW and SMC using IPv6

Engines that only use IPv6 to connect to the Internet can now be managed by SMC over the Internet using IPv6-based management connections. Connectivity between SMC components still requires IPv4 addressing and connectivity.

Network Security for Industrial Control Systems (ICS)

ICS support has been enhanced with deep inspection support for DNP3 (TCP/UDP) and Open Platform Communications Unified Architecture (OPC UA).

Safe search support

Stonesoft NGFW can be configured to enforce safe search usage for Google, Bing, Yahoo, and DuckDuckGo web searches.

Enhancements

This release of the product includes these enhancements.

Enhancements in Stonesoft NGFW version 5.10

Enhancement	Description
Advanced Threat Defense communication logging improvements	Improvements have been made to the communication protocol and logging features between McAfee® Advanced Threat Defense and Stonesoft NGFW. Stonesoft NGFW now logs the dynamic analysis results when available from Advanced Threat Defense. Stonesoft NGFW provides the file name, destination IP address, and URL details when sending the file to Advanced Threat Defense for analysis.
File filtering improvements	Improvements have been made to file type detection and filtering. We recommend that you update your file filtering policies with the new file type categories.
DHCP services	It is now possible to use DHCP server and DHCP relay services on different interfaces of the same Stonesoft NGFW engine.

Enhancements in Stonesoft NGFW version 5.10.3

Enhancement	Description
Dynamic routing enhancements	Dynamic routing features, such as graceful restart for OSPF and BGP, have been improved. The stability of dynamic routing has also been improved.

Enhancements in Stonesoft NGFW version 5.10.4

Enhancement	Description
Improved alerting for offline transitions	Alerting for offline transitions has been improved. Alerts are now created for unexpected offline transitions, such as heartbeat recovery, or nodes that have different policies.
Faster policy installation for Virtual Security Engines	Policy installation is now faster in environments that have many Virtual Security Engines.

Enhancements in Stonesoft NGFW version 5.10.8

Enhancement	Description
Engine monitoring enhancements	Engine monitoring has been improved. If the monitoring connection through a primary Control Interface fails, the backup Control Interface is used.
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.
Inspection with a larger number of Virtual Security Engines	Inspection can now be used with a larger number of Virtual Security Engines that are hosted on a single Master Engine.

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
SYN flood protection might consume too much memory.	FW, IPS, L2FW	NGFW-275
User information provided by McAfee Endpoint Intelligence Agent (EIA) overrides user information from user authentication, such as authentication using the Stonesoft VPN Client or Browser-Based User Authentication.	FW	NGFW-352
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 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
DHCP relay might stop working when you modify a VLAN Interface that has DHCP Relay enabled.	FW	NGFW-1274
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
QoS cannot be applied to multicast traffic.	FW	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	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
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

Description	Role	Issue number
The engine might not be able to decrypt HTTPS traffic from Google applications on Android devices.	FW, IPS, L2FW	NGFW-2116
On engines that have a large number of Physical Interfaces or VLAN Interfaces, Aggregated Link Interfaces might not work correctly.	FW	NGFW-2340
The engine might restart when VoIP connections are processed using the SIP Protocol Agent.	FW, IPS, L2FW	NGFW-2509

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 **Security Engine 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 5.10.x is only supported from version 5.8.x or later. If you have an earlier version, first upgrade to the latest 5.8.x version.
- Stonesoft NGFW 5.10.x requires an updated license if upgrading from version 5.9.x or earlier. 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*.

Take the following software architecture information into consideration.

- Stonesoft NGFW appliances support only the software architecture version with which they come installed. 32-bit versions (i386) can only be upgraded to another 32-bit version and 64-bit versions (x86-64) can only be upgraded to another 64-bit version.
- Clusters can only have online nodes that use the same software architecture version.
- State synchronization between 32-bit and 64-bit versions is not supported.
- Changing the architecture of third-party servers using software licenses requires the software to be fully re-installed from CD.
- Stonesoft NGFW version 5.10 only supports 64-bit software architecture. Except for the FW-315 appliance, the last supported software version for 32-bit Firewall/VPN appliances is 5.8.
- To upgrade a cluster (consisting of FW-315 appliances or third-party hardware using software licenses) from a 32-bit to 64-bit version, see Knowledge Base article 9875.

Known issues

For a list of known issues in this product release, see Knowledge Base article 10138.

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.
SSL/TLS inspection in capture (IDS) mode	Due to SSL/TLS protocol security features, SSL/TLS decryption in capture (IDS) mode can only be applied in a server protection scenario when RSA key exchange negotiation is used between the client and the server.
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.

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*