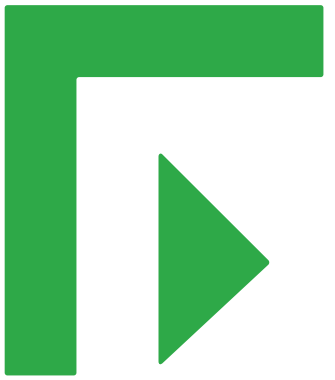

FORCEPOINT

Stonesoft Next Generation Firewall

Release Notes

5.10.8

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 in the product name in this document. However, the old product name is still used in the NGFW appliances, the NGFW engine software, 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 5.10.8 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 5.10.8 build version is 14103.

Product binary checksums

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

- sg_engine_5.10.8.14103_x86-64.iso

```
SHA1SUM:
13b966c1375c713ecbe76788ff8df925a47b58f2

SHA256SUM:
1d2121a47fb9b7859d330ebe5b74ad4d2eb39704efed2b70b35ea0e6e11ff064

SHA512SUM:
2150087f2b3339bb3e70d8f78c866d54
b4c190577929248fe8bb48f1dbdc1dea
c3933527f425536bc105ca698809e5d8
beed4205de52f50a2eb21468988c5732
```

- sg_engine_5.10.8.14103_x86-64.zip

```
SHA1SUM:
de50977033e3d58639ab4b16b630143e2d48b76b

SHA256SUM:
3339248c25b21d4f01e69db931e93b0526c84314813c9bd853ccf9773ec10999

SHA512SUM:
a78519c89c46391926de339aa14a59d3
de5da7698fb274d966a7cda5d6b9ca83
5692cf45201e08919edf4bc5b65318c9
6299422fc0c4d26782bc6d516ec3568d
```

- sg_engine_5.10.8.14103_x86-64-small.iso

```
SHA1SUM:
8d428657af8e5503fec95b711fc9e2e8d81a905a

SHA256SUM:
6494dc0ea5e1bb17bd35951c655eb3d6e89a664d6032d5a7a6187efe1957f1d3

SHA512SUM:
6277c2fb80cf2a2167a31f68e0ff40e2
2aa7356cd3d9f301784da9a9d74d93c2
6f93a19f7701a92e81cd2aeaa2171c9a
b6f34fd2c04c8ef12fad4e9814691449
```

- sg_engine_5.10.8.14103_x86-64-small.zip

```
SHA1SUM:
34681c3892b9ea1ae32e24b78f4adcf2ed9f429e

SHA256SUM:
83617449730e33b76d8aa588935405041c7aa33e1478bebf169fca81da7bf172

SHA512SUM:
76eef483b651fda995b25997262f30ca
e86099e263a07680679a664da2093080
26e7373b36a6b6a8b439a06b6cf511cf
5f32932396a61384416aeebde3881e7c
```

Compatibility

Stonesoft NGFW 5.10.8 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 5.10.8 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
When you upgrade FW-315 appliances to NGFW version 5.10, the engine architecture is changed from 32-bit to 64-bit. Because of the change in engine architecture, password authentication for users in the InternalDomain LDAP domain might not work after the upgrade.	FW	118371
When connections match an Access rule in which the Log Level is Alert and logging for Connection Closing is enabled, the engine might restart.	FW, IPS, L2FW	125020
The Master Engine might stop resolving DNS names used in the policy when the policy for a Virtual Security Engine is updated.	FW, IPS, L2FW	131081
NAT might not be correctly applied to REFER SIP messages by the SIP inspection module.	FW	132823
When the engine acts as an area border router (ABR) for an OSPF not-so-stubby area (NSSA), the engine does not correctly translate incremental changes from a type 7 link-state advertisement (LSA) to a type 5 LSA.	FW	133430
When VPN Client session handling is moved from one node in a cluster to another node, Virtual IP Address renewal for VPN Clients might not work correctly.	FW	134149
In rare cases when you have created a /data/config/base/file_decomp.conf configuration file, and the file contains the line "decompression_enabled=0", the inspection process might restart when a .zip file transfer is detected. Connections that are being inspected might be interrupted.	FW, IPS, L2FW	134379
The engine might log unnecessary SOFA errors when ATD is used.	FW, IPS, L2FW	134391
The engine might not receive all file reputation scan results from ATD. The following message might be shown in the logs: "error RESTQ:Bulk response JSON parse error: '[' or '{'expected near '<'."	FW, IPS, L2FW	134482
After restarting the engine, there can be a delay before Access rules that have a Domain Name element in the Source or Destination cell match traffic. As a result, some connections might match the wrong rules.	FW, IPS, L2FW	134532
When deep inspection or anti-malware is used in large environments, the engine might not process HTTP traffic efficiently. As a result, traffic throughput might become slow.	FW, IPS, L2FW	135156
The engine might not redistribute BGP routes through OSPF after changing the prefix list.	FW	135281
When there are a high number of new connections through dynamic NAT, the engine might slow down and print "BUG: soft lockup" messages to the console.	FW	135444
VPN Client session synchronization in clusters might not synchronize all information reliably. This issue can cause random failures in matching VPN Client connections to the Access rules.	FW	135527
When using IKEv2 and when more than one node in the cluster is in the online state, IPsec SA delete messages might not be sent correctly.	FW	135643

Description	Role	Issue number
In log entries for connections that are detected on Capture Interfaces, the Physical Interface information might be incorrect.	IPS	135657
The kernel has been updated to mitigate the TCP weakness described in CVE-2016-5696.	FW, IPS, L2FW	NGFW-115
The engine might restart when inspection is used.	FW, IPS, L2FW	NGFW-218
The OpenSSL library has been updated to mitigate the denial of service issue described in CVE-2016-6304.	FW, IPS, L2FW	NGFW-267
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
When you add a new Physical Interface or VLAN Interface to the engine, the SNMP agent on the engine might stop listening.	FW, IPS, L2FW	NGFW-541
When McAfee Logon Collector is used, the engine might unnecessarily log "SGE assertion failed" events. The incorrect logging can affect the processing of traffic, and some traffic might be stopped.	FW, IPS, L2FW	NGFW-694
If you change the MTU to a value other than the default value on an interface that has an IPv6 address, you might not be able to refresh the policy or monitor routing for the engine.	FW	NGFW-891
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
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
If the user that is being authenticated belongs to a large number of User Groups, user authentication might be slow or might not work.	FW	NGFW-1279
Inspection of HTTP or HTTPS traffic might stop working.	FW, IPS, L2FW	NGFW-1309
On interfaces that use the MOD-EM2-10G-SFP-4/MOE10F4 or MOD-40G-2/MO40F2 interface modules, traffic might only work partially after you add a VLAN interface to an Aggregated Link interface.	FW	NGFW-1507

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*