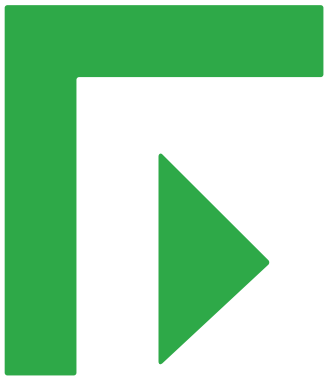

FORCEPOINT

Stonesoft Next Generation Firewall

Release Notes

5.10.3

Revision C

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.

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 10192 and Knowledge Base article 9743 for up-to-date appliance-specific software compatibility information.

Appliance model	Supported roles	Image type
FW-315	Firewall/VPN	x86-64-small
320X (MIL-320)	Firewall/VPN	x86-64
IPS-1205	IPS and Layer 2 Firewall	x86-64
FWL321	Firewall/VPN	x86-64-small
NGF321	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
FWL325	Firewall/VPN	x86-64-small
NGF325	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
110	Firewall/VPN	x86-64-small
1035	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
1065	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
1301	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
1302	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
1401	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
1402	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64

Appliance model	Supported roles	Image type
3201	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
3202	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
3205	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
3206	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
3207	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
3301	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
3305	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
5201	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
5205	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
5206	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64

Sidewinder S-series appliances

These Sidewinder appliances can be re-imaged to run Stonesoft NGFW software.

Appliance model	Supported roles	Image type
S-1104	Firewall/VPN	x86-64
S-2008	Firewall/VPN	x86-64
S-3008	Firewall/VPN	x86-64
S-4016	Firewall/VPN	x86-64
S-5032	Firewall/VPN	x86-64
S-6032	Firewall/VPN	x86-64

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 5.10.3 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 5.10.3 build version is 14084.

Product binary checksums

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

- sg_engine_5.10.3.14084_x86-64.iso

```
SHA1SUM:
a09ab62304e0de721dff7ad51ef9d88c5482efb2

SHA256SUM:
8d8ed43d37fa3f2af38568bd5fb69770f47ab830ac8261ae75e95f97516d41f7

SHA512SUM:
2e0e102a86214caca5f696eaa7800270
da918e68f33b8e1a50661366a5765c12
7d3df7001e6088f8466ea1b53561f0cd
c7be01ce73006f7c7ad13c5e0c70a47e
```

- sg_engine_5.10.3.14084_x86-64.zip

```
SHA1SUM:
60af2ea28857ed3d7db8bdcf982776b6cd31b384

SHA256SUM:
200e197e64f0bf5061c0268233a73f8b6ee051ad255ee628f5202d0bad53fbfb

SHA512SUM:
e0b3f4a051b7528c6a6aa390544d716e
abb1e560d0421519f229b0c975f4f4b2
3eebc255a0313022cad19a45262f13e4
a490f6cad327f66365f8542d5cc9b577
```

- sg_engine_5.10.3.14084_x86-64-small.iso

```
SHA1SUM:
1139cadda7b9b541b417e81213d2f8410d988bcd

SHA256SUM:
2713009774e46bd2d1ad2ab5e8a3ae065849987a81d55a566d772168bb949197

SHA512SUM:
182215532750aaac7ecfe9bd1cefb627
db753006740c88a3388250455b77d6ea
de5253c9635483f3aa533d30800299bd
9be2bfcf6652bfd7a7ba7dd27411e5d5
```

- sg_engine_5.10.3.14084_x86-64-small.zip

```
SHA1SUM:
7762b6aee8a52d29c73d99b75f4c5fa33f7f3ead

SHA256SUM:
f6d9956c7494da122026f60b6a979fd05b1087595ec301cb82307a36a4305e37

SHA512SUM:
48b1826f654b1d26c5aeb2d2c2363101
5f6b574e269fb5f6d84bbb02ec812070
65ad72346de0792d7db2415b0a876f9c
92fb0fc4ee24c5966ad97f9f3f55d159
```

Compatibility

Stonesoft NGFW 5.10.3 is compatible with the following component versions.

- McAfee® Security Management Center (SMC) 5.10.0 or later
- Dynamic Update 703 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 3.0
- McAfee® Endpoint Intelligence Agent (McAfee EIA) 2.5

New features

This release of the product includes these new features.

Note: Stonesoft Next Generation Firewall 5.10.3 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.

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 internal DHCP Server cannot be used for more than one Virtual Firewall Engine at a time on the same single node Master Engine.	FW	116348
The engine might incorrectly drop HTTP proxy connections. The matched Situation is "HTTP_SHS-Invalid-Response-HTTP-1.0". The default action for this Situation is Terminate.	FW IPS L2FW	117048
FW-315 appliances might restart unexpectedly after upgrading from version 5.x to version 5.9.0 or higher.	FW	119193
The inspection process might restart when using a File Filtering Policy.	FW IPS L2FW	120193
The inspection process might restart when using Users or User Groups and Correlation Situations in the same rule in the Inspection Policy.	FW IPS L2FW	126022
Virtual Security Engines might be deleted during policy installation if there are problems with interface mapping.	FW IPS L2FW	126344
The engine might reply to SNMP queries slowly if an ADSL interface is configured and in use.	FW	126792
IPv6 routes learned through dynamic routing are not synchronized between nodes.	FW	127479
"Connection Closed" log entries do not include VLAN information in the "Src VLAN" and "Dst VLAN" fields. As a result, statistics items such as "Traffic by Src VLAN" are empty.	FW IPS L2FW	127815
A Virtual Security Engine might stop processing traffic for a short time when the engine is moved from one Master Engine node to another during failover.	FW	127921
Only Virtual Firewalls running on single node Master Engines support DHCP server configuration. Master Engine clusters incorrectly allow DHCP server configuration for Virtual Firewalls. This fix prevents the incorrect configuration by denying policy upload with the following error message: "Error: DHCP server cannot be configured with virtual context when using more than one master engine node".	FW	127953
A Virtual Security Engine might not be moved from one Master Engine node another when the move is done manually.	FW IPS L2FW	128009

Description	Role	Issue number
Traffic might be balanced unevenly between physical interfaces in an aggregated link interface if it has a VLAN interface assigned.	FW	128047
The engine might reply with incorrect ifHCInUcastPkts counter values for SNMP queries.	FW IPS L2FW	128195
File filtering does not work for IPv6 traffic if IPv6 addresses are used in the File Filtering Policy.	FW IPS L2FW	128213
Policy installation might fail when there is a large DHCP relay configuration. When upgrading to version 5.10, the engine might go to the initial configuration state if the DHCP configuration is large enough. Policy installation fails and the following error message is shown: "FATAL: Sending configuration to dhcps failed (error -5)".	FW	128369
The engine might occasionally stop processing traffic if there is more than one multicast router in the same LAN segment and IGMPv2 is used.	FW	128498
When Virtual Security Engines roll back due to problems with policy installation, the engines might sometimes roll back to the wrong policy.	FW IPS L2FW	128678
Anti-spam might not work.	FW IPS L2FW	128833
Adding an IPv6 address to the list of Loopback IP Addresses configures that address with the wrong prefix, and causes IPv6 routing to fail.	FW	128914
The engine might unnecessarily create files in the /spool/av/scan directory when using a File Filtering Policy.	FW IPS L2FW	128917
The inspection process might restart when using DoS protection.	FW IPS L2FW	128989
The engine might incorrectly change DSCP marks for packets.	FW	129052
When the engine has not received a scan result from ATD within 4 seconds, the engine might send an incorrect cancel scan request to ATD. The scan result is not cached on the engine, and the following message is shown in the logs: "ATD responded with error 7 for file_id:".	FW IPS L2FW	129055
The engine might unnecessarily log "SGE assertion failed" events. The incorrect logging might affect traffic processing, and might cause part of the traffic to fail.	FW IPS L2FW	129245

Description	Role	Issue number
The engine might stop processing traffic in SSL VPN tunnels if TLS inspection or a File Filtering Policy is applied to the traffic.	FW	129292
The engine does not accept DHCP messages that are smaller than 300 bytes. Some common devices send these non-standard messages.	FW	129325
The engine might restart when authentication is applied to connections that are allowed without connection tracking.	FW	129342
The engine might stop processing traffic when using TLS decryption and file filtering.	FW IPS L2FW	129441
The engine might incorrectly drop TCP packets when the TCP checksum is 0xffff. The matching Situation that terminates the connection is "TCP_Checksum-Mismatch".	FW IPS L2FW	129503
NIC detection might fail on S-series appliances after upgrading to versions 5.10.0, 5.10.1, or 5.10.2. The upgrade causes the interfaces to be mapped differently. Features that get information from NIC detection, such as the Monitoring view in the Management Client, no longer show the interfaces.	FW IPS L2FW	129823
QoS might not be applied correctly for HTTP traffic when file filtering is enabled in the same Access rule.	FW IPS L2FW	129991

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 the following Knowledge Base article: 81935.

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

The following documents included in appliance deliveries still use the old product name and brand:

- *McAfee Security Management Center Appliance Quick Start Guide*
- *McAfee Next Generation Firewall Quick Start Guide*