



FORCEPOINT

Stonesoft Next Generation Firewall

Release Notes

5.10.4

Revision C

Table of contents

- 1 About this release.....3
 - System requirements..... 3
 - Build version.....6
 - Compatibility.....7
- 2 New features.....8
- 3 Enhancements.....9
- 4 Resolved issues..... 10
- 5 Installation instructions.....11
 - Upgrade instructions..... 11
- 6 Known issues.....12
 - Known limitations..... 12
- 7 Find product documentation..... 13
 - Product documentation..... 13

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 5.10.4 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 5.10.4 build version is 14087.

Product binary checksums

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

- **sg_engine_5.10.4.14087_x86-64.iso**

```
SHA1SUM:
a534e2dd5cd1c3f8034a9053d68c1e938840614f

SHA256SUM:
262c9c7ebc82a14c9dfe1e9161437668eca5e9f8beca5889d004f7769c1a49a7

SHA512SUM:

12db2da34de9796a2fa25e687ae82643
a70e9ecc59740f4232faf5e663a7a93f
e9a1e0a6a0ac184e0305a6847993759e
1278658fc9f1f2d52266b42bc2ad29b3
```

- **sg_engine_5.10.4.14087_x86-64.zip**

```
SHA1SUM:
838dacc4b3a7edab97c6be54f257ee89d06ee8b2

SHA256SUM:
55fe7045645b47bdb9e8c60d7d5f3850ce3c014489cd1aaf9d1a89a391f2a41d

SHA512SUM:

ecc0d05455d5ae9ea3725b6ba82d8774
4e33edc3d56375dc602f1f2abbbb3569
c54bef6a18ccb0c3a06a80fc76bac841
2b7facd45651881a631aa3c2ba9c3d72
```

- **sg_engine_5.10.4.14087_x86-64-small.iso**

```
SHA1SUM:
e49f8d62657c284dc0aa4c2692da2017bdf69c32

SHA256SUM:
762317a35fb0281f2f86f765a0eb5e9380e97c13c034c3047402c9b6643bd606

SHA512SUM:

ab740367d490a075a3e76145447d3ea5
73a6436430474a90b41a4f3b48e8403b
facb17231eb409c1654a0cb1c46f4a15
908626809db696719fbdddb18587050c
```

- sg_engine_5.10.4.14087_x86-64-small.zip

```
SHA1SUM:  
c0e225f1f42737922512e4c30128791eb3406056  
  
SHA256SUM:  
eeb4aa06993020036d5c9bec3b5064d825e78b6a966a1aa8d78cf13e02bd3a6d  
  
SHA512SUM:  
  
2c180ba81539114c745e6caa2954238a  
71ae39cdf5cb55c636f7655470129b8  
4c7710245f83570010c0c3d7103cadca  
62ce35950deac3b98a4dcd455704ed5d
```

Compatibility

Stonesoft NGFW 5.10.4 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 5.10.4 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.

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
A tunnel interface might disappear from a Virtual Security Engine if the Tunnel Interface ID is changed in the Management Client and the policy is refreshed.	FW	125308
The engine might not log all SYN and SYN-ACK packets that are dropped due to incorrect TCP options.	FW IPS L2FW	127436
"Src Zone" information might be missing in log messages related to packet validity check Situations such as "TCP_Segment-SYN-No_Options".	FW IPS L2FW	129402
The engine might go to the initial configuration state after an upgrade when SSL tunnels for VPN clients are used.	FW	130337
The engine might reboot when CIS redirection and Multi-Link NAT are applied to the same connection.	FW	130522
DNS might not be configured correctly on Master Engines when some of the Virtual Security Engines have DNS configured. As a result, features such as URL filtering and anti-malware might stop working.	FW IPS L2FW	130661
The engine might not handle SIP traffic correctly when load-balanced clustering is used. The issue causes RTP traffic to fail.	FW IPS L2FW	130721
The engine might restart when fragmented traffic uses the route-based VPN and the engine is part of a cluster.	FW	130739
The engine might restart when deep inspection is used.	FW IPS L2FW	131028
The dynamic routing process does not start on Master Engine clusters that use load-balanced clustering.	FW	131046

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 <i>disconnect mode</i> 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*