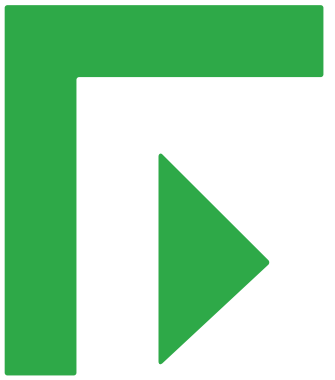

FORCEPOINT

Stonesoft Next Generation Firewall

Release Notes

5.10.6

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.

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 5.10.6 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 5.10.6 build version is 14094.

Product binary checksums

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

- sg_engine_5.10.6.14094_x86-64.iso

```
SHA1SUM:
6ef21e3efd6daec18cd9b6a3bf966a6fda392baa

SHA256SUM:
bdf9c66975d1c24fcfe618c1f2038e97ff235308c312a3c389f3d07cb1a3ce44

SHA512SUM:
52a5482f35affc76de429d71427b2696
aab6cd4ea783f8d2ddef56075a79eed2
8f459da00f0a16b3dfea8775434d8641
9003a6805dea78931456bc017e6213b1
```

- sg_engine_5.10.6.14094_x86-64.zip

```
SHA1SUM:
0436bced7022a3e99c30ab441e1d0f294dd140fd

SHA256SUM:
6aa05eef16b84ebf5aa945043426a55949b228aa9fcb736f838e1ebff58588d8

SHA512SUM:
1a43f93a2c34748857603b48dbd6bfb9
9405e651662028e26814e2238ad4e7af
726c1ca0ad5e097c6aa15be405c05ba5
7edf2af1b28a9fc18202cc75b81da836
```

- sg_engine_5.10.6.14094_x86-64-small.iso

```
SHA1SUM:
f6010213c6a7b52db27a257bf2c31ffb52a0537d

SHA256SUM:
7caf78584e406431377d7729a75c4ef325283321efcc9fc5fb7cf7bbc8c63795

SHA512SUM:
80ee45a3b239a015442d588a00b0718b
50a6c681a2b1586f70e51389498de48e
d83750a40e540651c0068774bbfe396c
7e260111ff7c911cb60ac03e95e6cd9a
```

- sg_engine_5.10.6.14094_x86-64-small.zip

```
SHA1SUM:
71f440af6cacdebed971c646ce1755defdf83559

SHA256SUM:
1be36358d476a2559ff2dd6455f530d25a2254f4c8a74c9a5172a66d1001f5bf

SHA512SUM:
e3e66511c61d2571cf32f997f3297b11
d59877afa723fb1059297776e651ea90
53df41f960a24b9e5b676aa6f4b14a70
4184c939c896814ab24e9d20364b8740
```

Compatibility

Stonesoft NGFW 5.10.6 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 5.10.6 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
The authentication timeout defined in the Authentication field of an Access rule is not applied to connections that also match a NAT rule that has a User or a User Group in the Source field. Instead, the default timeout of one hour is applied.	FW	116964
If loose connection tracking and inspection are applied to connections, TCP connections might not be closed correctly. As a result, the closed connections remain in the engine's state table in the established state. The incorrectly closed connections might prevent connections that use the same ports from being established.	FW IPS L2FW	120185
Route-Based VPN tunnels might stop working after unrelated VPN configuration changes. Symptoms include packets dropped with log messages such as "spoofed VPN tunnel [vpn_id[1]=0 vpn_by_tunnel_id=12, tunnel_id=3]" or "spoofed packet. NIC index asymmetry. The packet did not come through correct NIC. (expected index=4 but came from index 14, name=vpn43, packet->dev=vpn43)".	FW	130506
When a node in a cluster restarts in environments with large VPN configurations, the node might go online before all VPN related data is synchronized between the nodes. As a result, part of the VPN traffic might fail right after the restart.	FW	131271
The engine might not react quickly enough when the IGMP querier changes if there is more than one multicast router in the same LAN segment. As a result, multicast traffic might stop working until the engine reacts to the changes and becomes the new IGMP querier.	FW	131368
TLS decryption might fail if the client and server use unsupported TLS cipher suites. The following log entry might be seen: "TLS_Unrecoverable-Error".	FW IPS L2FW	131780
When the Proxy ARP setting is selected in the VPN Client settings for the engine, the engine also sends gratuitous ARP for virtual IP addresses that are not currently in use.	FW	132355
In rare cases when both protocol identification and file filtering are applied to the traffic, the engine might not forward traffic correctly.	FW IPS L2FW	132578
TFTP traffic might not be handled correctly if TFTP connections are allowed with ANY Service instead of the TFTP Service. As a result, connections are terminated and the following log entries might be seen: "TFTP_Read_Violation", "TFTP_Write_Violation".	FW IPS L2FW	132612
ATD results might be reported differently in the NGFW logs compared to the ATD server.	FW IPS L2FW	132623

Description	Role	Issue number
The engine might stop sending files to ATD if the message sent by ATD to the NGFW engine is too long and the engine cannot parse it.	FW IPS L2FW	132630
The engine might become unresponsive when ATD is temporarily under a heavy load and cannot handle all files sent by the NGFW engine.	FW IPS L2FW	132636
VPN Client connections through SSL VPN tunnels might occasionally fail. The following log entry might be seen: "Could not resolve tunnel id for 2nd level".	FW	132649
NAT might not be applied correctly to all SIP traffic due to parsing errors on the engine. The following log entry might be seen: "SIP_Message-Parse-Error".	FW	132820
GRE or IP-IP traffic passing through a route-based VPN tunnel with the VPN tunnel type might be dropped. The following log entry might be seen: "spoofed packet. NIC index asymmetry. The packet did not come through correct NIC."	FW	132897
When using DHCP relay, the engine sends DHCP offer messages with 0.0.0.0 as the source address instead of its IP address if the broadcast flag is set on the DHCP request.	FW	133138
The NGFW Multi-Link VPN probe is triggered in single-link VPN tunnels with third-party gateways. In large VPN configurations, the VPN process might stop working, and part of the VPN traffic might fail.	FW	133142
In rare cases when HTTP traffic uses a non-standard port, the inspection process might restart. As a result, inspected traffic might stop working.	FW IPS L2FW	133612
The engine might restart when log rate limiting has been configured in one or more Access rules.	FW IPS L2FW	133935
When Virtual Security Engines are used and more than one Master Engine node is online at the same time, VPN Client connections that use external LDAP authentication might not work.	FW	133941

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*