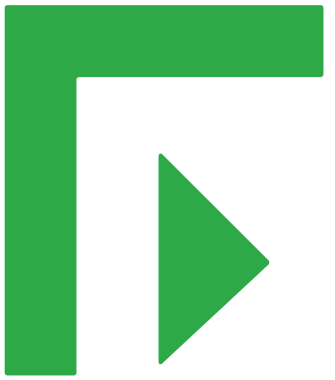

FORCEPOINT

Stonesoft Next Generation Firewall

Release Notes

5.10.2

Revision A

Table of contents

About this release

This document contains important information about the current 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.

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 end-of-life support and KnowledgeBase article KB78906 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
3201	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64
3202	Firewall/VPN, IPS, and Layer 2 Firewall	x86-64

Appliance model	Supported roles	Image type
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
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

Certified Intel platforms

We have certified specific Intel-based platforms for Stonesoft NGFW.

The tested platforms can be found in the ServicePortal (https://support.mcafee.com) under the 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 KnowledgeBase article KB78844.

Master Engine requirements

Master Engines have specific hardware requirements.

- Each Master Engine must run on a separate physical device. For more details, see the *McAfee 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 *McAfee 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: Deployment on VMware NSX is supported only with Intel® Security Controller (Intel Security Controller) integration.
  - 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.

Intel Security Controller integration

Systems must meet these requirements to install Intel Security Controller.

- Intel® Security Controller version 2.0
- VMware components and versions:
  - vCenter 5.5
  - vSphere web client
  - NSX 6.1.4 or 6.2.0
  - ESXi 5.5
  - Each firewall engine deployed by Intel Security Controller uses these resources:
    - 4 CPUs

- 8 GB of memory
- 20 GB of the datastore capacity

Build version

Stonesoft Next Generation Firewall 5.10.2 build version is 14076.

Product binary checksums

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

- sg_engine_5.10.2.14076_x86-64.iso

```
SHA1SUM:
3b94791ea4f4cf82cf4b7cdaebdcc33e5cbbf451

SHA512SUM:
5052cf26e101048f064353805600d2ce
d8172e17f577dd33da0aa30839c59851
ba42f7f9a4bd78783735a014fff73d35
49d4d51ce8555fc26be9f6a4022df56a
```

- sg_engine_5.10.2.14076_x86-64.zip

```
SHA1SUM:
a60081e062fab9d358d98e57025e1c5d0ad97f23

SHA512SUM:
9200924d11c148285096a2b030ac96f5
ed74edab556a1392b51563367e728e53
ecff44c1d59df1a484c34de7c84a5f38
9131f5156c9cd1b75c89493abdc2341f
```

- sg_engine_5.10.2.14076_x86-64-small.iso

```
SHA1SUM:
e7d331607e83ff96062a22c3db642718b5117874

SHA512SUM:
5bd22a8ffd7b2c7a04043c48cab6f7f1
7a65d481898b333ec72dcc1ab3c443a5
031b4c8113e82eb3d6f399eefd458696
ffe2d008b01d7917ce7501854f86e872
```

- sg_engine_5.10.2.14076_x86-64-small.zip

```
SHA1SUM:
09636d39bc9b1bb21ed0b5c753cc2899b154514b

SHA512SUM:
d15bb8143d39f5ce329d57245868013e
c8d75444fee5033da90147ce941276d5
73a099d4b5bafda19a8309b5342745a9
8608b979ee149bb448a761ab7127028f
```

- McAfee-NGFW-nsx-5.10.2.14076.zip

```
SHA1SUM:
74a239298a5ab36a1260ef9717476f805080d789

SHA512SUM
a506d4d477bfefafbc13b09994546cd2
de3bc7452e0986c67ffe27a5e9f2a0b0
2be741388166881d7f1294e512caefa9
25eb401deb9a89c4af1d52900ec6c874
```

McAfee-NGFW-nsx-5.10.2.14076.zip contains the VSS Context Firewall engine image that is used with Intel Security Controller. For more information, see the *McAfee Next Generation Firewall Product Guide*.

Compatibility

Stonesoft NGFW 5.10.2 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

Note: Engines deployed through the Intel Security Controller integration are not compatible with McAfee EIA.

New features

This release of the product includes these new features.

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.

Support for Intel Security Controller and VMware NSX

Intel Security Controller is a management service that coordinates between Stonesoft NGFW and virtualization platforms. It allows the rapid deployment and provisioning of engines across a diverse virtual network. Traffic can be filtered on the perimeter of the network and within it.

Enhancements

This release of the product includes these enhancements.

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.

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 an interface has been assigned to a Virtual Security Engine and it has VLANs configured, interface monitoring for the VLAN interface might not work.	FW IPS L2FW	101773
Log data from Virtual Security Engines might contain wrong VLAN IDs or show "0" for the VLAN ID.	FW IPS L2FW	102577
The engine might run out of memory, which can cause the engine to hang or restart, when its connections are monitored in the Connections view in the Management Client.	FW IPS L2FW	106840
Scan detection might fail to detect connections with invalid TCP packets even though the packets themselves are detected by the engine.	FW IPS L2FW	113344
DoS protection might not send RST packets to close connections if deep inspection is applied to the connections.	FW IPS L2FW	113445
A File Filtering Policy might not handle email protocols correctly. It might block email connections instead of blocking attachments.	FW IPS L2FW	114447
Logs generated by Inspection rule matches might not include information such as the User and QoS Class. This might cause certain Report and Overview items to show inaccurate data.	FW IPS L2FW	116223
The engine does not send to the Log Server the details of a virus that an ATD server has detected. As a result, the Malware field in the Logs view in the Management Client is empty.	FW IPS L2FW	116428
A Master Engine that is online might reboot when you run the sg-reconfigure command.	FW IPS L2FW	116699
In rare situations, the Security Engine might reboot when Multi-Link is in use.	FW	116755

Description	Role	Issue number
Related connections allowed by the Protocol Agent might be inspected even if deep inspection is not enabled.	FW	116857
If you start sg-reconfigure while a node is still online, existing network interface card ID mappings in the sg-reconfigure "Configure Network Interfaces" screen might be incorrect. The issue does not affect modular NGFW appliances.	FW	117139
A CVI MAC address might not be added correctly to an aggregated interface if there is only one node configured within a cluster.	FW	117153
The Security Engine might log "System_Engine-NIC-Dropped-RX-Packets" Situations unnecessarily.	FW IPS L2FW	117183
A Virtual Security Engine does not send gratuitous ARP messages for proxy ARP addresses if the Virtual Security Engine is switched from one Master Engine to another and a cluster MAC address is not defined on the Master Engine.	FW	117258
The inspection process might restart or in some situations hang when a File Filtering Policy is in use.	FW IPS L2FW	117314
HTTP proxy connections might not be handled correctly when HTTP safe search is in use.	FW IPS L2FW	119900
A GRE tunnel cannot be established if the endpoints use IPv6 addresses.	FW	120020
A PPPoE tunnel might fail on the engine after the initial contact in sg-reconfigure.	FW	120061
When Anti-Malware is in use, connections through the engine might be delayed if the engine is still downloading signature files for the first time when connections arrive to the engine.	FW IPS L2FW	120166
Policy installation might fail if the engine has an interface with a dynamic IPv6 address, but no DHCPv6 server is available.	FW	120203
The engine might leave unnecessary files under /spool/av/scan when a File Filtering Policy is in use.	FW IPS L2FW	120244
The engine might not handle IPv6 FTP connections correctly if the FTP Protocol Agent is used in Access rules and NAT is applied to the connections. This issue does not happen if the IPv6 FTP connections are also inspected.	FW	120306
The DHCP relay feature does not work with DHCP servers that drop the relay agent information option from the DHCP messages.	FW	120314
The engine might allow files through when Global Threat Intelligence (GTI) is used and connectivity with the GTI server is lost, even if "Action when file cannot be scanned" is set to "Discard" in the File Filtering Policy.	FW IPS L2FW	124610

Description	Role	Issue number
The Virtual Security Engine might be deleted during the policy installation if there is non-matching interface mapping. This can happen when an interface is added to the Virtual Security Engine and the policy is installed on the Virtual Security Engine, but not installed on the Master Engine.	FW IPS L2FW	124640
TCP connections that have the timestamp option set might not work if they are matched against the File Filtering Policy and TCP retransmit is seen within the connection.	FW IPS L2FW	124656
In situations where a Virtual Security Engine has an IPv6 NAT rule configured, if the Master Engine is restarted, the engine might end up in a restart loop.	FW	124667
Dynamic routing might stop working if the Lock Online command is sent to the engine.	FW	125000
Interfaces that are assigned to a Virtual Security Engine cannot be seen in sg-reconfigure on the Master Engine. As a result, some settings, such as speed/duplex settings, cannot be changed.	FW IPS L2FW	125057
The full URL might not show in the URL log field, even if URL logging is enabled.	FW IPS L2FW	125360
The logs for new SSL VPN Portal connections might show incorrect source addresses.	FW	125414
Multipath routes cannot be synchronized between nodes in a Firewall Cluster. As a result, dynamic routing might stop working during failover situations.	FW	125681
The "Soft Reconfiguration Inbound" setting is not enabled for IPv6 if the setting is enabled through the Management Client.	FW	125870
The engine might restart itself in certain situations when inspection is applied to VPN connections.	FW	126745
The engine might not respond to SNMP requests in rare situations where the ARP cache has an exceptionally large amount of entries.	FW IPS L2FW	126747
The GLIBC library used in the NGFW engine is vulnerable to the issue described in CVE-2015-7547. This can affect the NGFW engine if the engine is configured to use an untrusted DNS server or if there is the possibility of a man-in-the-middle attack on DNS queries made by the NGFW engine. By default, no DNS servers are configured in NGFW engines.	FW IPS L2FW	127287

Installation instructions

Use these high-level steps to install SMC and the Stonesoft NGFW engines.

For detailed information, see the *McAfee Next Generation Firewall Installation Guide*. All guides are available for download at https://support.mcafee.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://ngfwlicenses.mcafee.com/managelicense.do.
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://ngfwlicenses.mcafee.com/managelicense.do. 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 *McAfee 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 KnowledgeBase article: KB81935.

Known issues

For a list of known issues in this product release, see KB85596.

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 **ServicePortal**, you can find information about a released product, including product documentation, technical articles, and more.

1. Go to the **ServicePortal** at https://support.mcafee.com and click the **Knowledge Center** tab.
2. In the **Knowledge Base** pane under **Content Source**, click **Product Documentation**.
3. Select a product and version, then click **Search** to display a list of documents.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *McAfee Next Generation Firewall Product Guide*
- McAfee 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 KB84639.
- *McAfee Next Generation Firewall Installation Guide*

Other available documents include:

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

Copyright © 1996 - 2016 Forcepoint LLC
Forcepoint™ is a trademark of Forcepoint LLC.
SureView®, ThreatSeeker®, TRITON®, Sidewinder® and Stonesoft® are registered trademarks of Forcepoint LLC.
Raytheon is a registered trademark of Raytheon Company.
All other trademarks and registered trademarks are property of their respective owners.