FORCEPOINT

Stonesoft Next Generation Firewall

Release Notes

5.10.1

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.

This NGFW engine version 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 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

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
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 5.10.1 build version is 14052.

Product binary checksums

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

- sg_engine_5.10.1.14052_x86-64.iso

```
SHA1SUM:
994eb020ab4ee6418deefcf68548dfdf656a7763

SHA256SUM:
c11a6e282df8ef6e
159431cd4b3c7b52
5252fb92f5929010
b74e1b965cfc4eb6

SHA512SUM:
1d51537d008914740426690c79f06dda
2b7f0b4a18fd7b76436a43071d93f84a
bc82c6c87b94c9c081c8080bcdf784d0
ca40444e5f9795e56a690c84503ad863
```

- sg_engine_5.10.1.14052_x86-64.zip

```
SHA1SUM:
e057073e9823874cf6ba6ea4bb42c64e0d8bb7b9

SHA256SUM:
40afe9b4846d8dbd
1708c12cb15d988b
15682ef6c17ce720
662021dd89203532

SHA512SUM:
bb9261a85898dc2efa8230ad4f162c1f
723e3d823b8d58e5215b1a7a0ef808e5
8b5a72022f2e149acefd6c3cdefdad62
51e8eaf5ab5e42d19e35d0c7f6ffe76f
```

- sg_engine_5.10.1.14052_x86-64-small.iso

```
SHA1SUM:
3a1940a0c4cb163762f78b647af3f88bd18a8333

SHA256SUM:
8d174f26a3da6f79
fef92a5831c7a55d
bcc3ebd9742a1e3f
7a296ce4f63d4273

SHA512SUM:
e7650b263c0b78c260c6782512c84753
3b8236b57c1973a1523b597c44bf5f44
b684dcc46edd8ca38737b5d53949a3b4
c706a11e0962fa5104a12bfbc7ad3dcb
```

- sg_engine_5.10.1.14052_x86-64-small.zip

```
SHA1SUM:
a8db532ad68da2283c0d50aa1a9ccc2fabad0fac

SHA256SUM:
7cbcc558d731eb5b
629b4225762df5b9
a6559c15a2a75e78
60573a890bb168bc

SHA512SUM:
99ae78dbc7978af1d5d0a55b772946a1
c3a8092f8f840300a0021709d50a1a99
8b411d6484a79775e729314c7ce6bb25
6008082bd896b4db496a13609a93edde
```

- McAfee-NGFW-nsx-5.10.1.14052.zip

```
SHA1SUM:
927dbc28546420246f1670f2931a0179a9daa8d3

SHA256SUM:
6747dc9cb8d9dc2a
9b7c84b6b2a8e8eb
311c5c3618b2665a
f0e30b2fcb945719

SHA512SUM:
aa08627bb92e1fc292c31926fb7474ab
18fac85faf3e6078de82e36f71255b22
1bf6652eec80593d937218e942d1da67
711d6334bbabe4c5c076bd1e3c2d4275
```

McAfee-NGFW-nsx-5.10.1.14052.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 5.10.1 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
Packet filter diagnostics do not include information on incomplete and invalid fragmented packets.	FW IPS L2FW	125580

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*