Release Notes

Revision B

McAfee Next Generation Firewall 5.10.0

Contents

About this release

This document contains important information about the current release of McAfee® Next Generation Firewall (McAfee NGFW). We strongly recommend that you read the entire document.

System requirements

Make sure that you meet these basic hardware and software requirements.

McAfee NGFW appliances

We strongly recommend using a pre-installed McAfee NGFW appliance as the hardware solution for new McAfee NGFW installations.

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

Appliance model	Supported roles	Image type
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
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

McAfee has certified specific Intel-based platforms for McAfee NGFW.

The tested platforms can be found in the McAfee Support Knowledge Center (https://support.mcafee.com/ServicePortal/faces/knowledgecenter) under the McAfee Next Generation Firewall product.

We strongly recommend using certified hardware or a pre-installed McAfee NGFW appliance as the hardware solution for new McAfee NGFW installations. If it is not possible to use a certified platform, McAfee NGFW can also run on standard Intel-based hardware that fulfills the hardware requirements.

Basic hardware requirements

You can install McAfee NGFW on standard hardware with these basic requirements.

- (Recommended for new deployments) Intel® Xeon®-based hardware from the E5-16xx product family or higher

  Legacy deployments with Intel® Core™2 are supported.

- IDE hard disk and CD drive

  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 McAfee 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

  Legacy deployments with Intel® Core™2 are supported.

- One of the following hypervisors:
  - VMware ESXi 5.5 and 6.0

    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 McAfee 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 McAfee 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

McAfee Next Generation Firewall 5.10.0 build version is 14045.

Product binary checksums

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

- sg_engine_5.10.0.14045_x86-64.iso

```
SHA1SUM:
a7558431d6eaa1e5fd7382e775d0382bb0a23908

SHA512SUM:
6a9906e668b6a39a7eb1c9604509c620
f5b54aaf2a81c511ea0a0e67807237ae
143ec9cd46ebd2a8952b7c9ea71bc10b
b53c7409d155c32448de3eca43652acf
```

- sg_engine_5.10.0.14045_x86-64.zip

```
SHA1SUM:
6426f645bd3d8dc60fb415567b8ad61d08f40fa3

SHA512SUM:
8d7a540d4cfdfdf4148782015d6bee5b
a92010b3c4a6d1ce7b326b8a87ce2a10
763f969167a91d850c2d340ff66e257e
2740df3b6d3f1dcb22e5dd9a6eb4e2cc
```

- sg_engine_5.10.0.14045_x86-64-small.iso

```
SHA1SUM:
ae1ec93e039c561837746f4a7de1b0c8945c06c3

SHA512SUM:
64f933f8b34486326cb26ff11546c294
04929ff7d6c3de9fff9e15bbb73c2ada
c7ca59b4579dfeea6c447818dd71f996
60e6d7b35ca2558b7c9a3e661f5985c7
```

- sg_engine_5.10.0.14045_x86-64-small.zip

```
SHA1SUM:
10aa58a1ed3908e66efdcc1a501e4a904f467527

SHA512SUM:
1237d052013e14129904d31e6e752735
bc848083780ac54064413dbacbf357c4
347426a31920e8605327b013bde1f29b
5eb01e06b3c595a232bf2e5c777c9fe4
```

- McAfee-NGFW-nsx-5.10.0.14045.zip

```
SHA1SUM:
4d2018d40c51ab7dbaf44ba9a27431ef494ba462

SHA512SUM:
50fcc9ca3c572d2b03a7b8b81a9b4bac
f7668957bea4863494e3e5c1d0d15447
6bfc3c1463625870c7d93043de5d2244
2ed0cc82c93f2657ccd221bafc9a8b21
```

McAfee-NGFW-nsx-5.10.0.14045.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

McAfee NGFW 5.10.0 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

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

McAfee 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 McAfee 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 has been improved.

Connectivity between McAfee 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).

Google SafeSearch support

McAfee 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 McAfee 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 McAfee NGFW. McAfee NGFW now logs the dynamic analysis results when available from Advanced Threat Defense. McAfee 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 McAfee 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
A cluster node might incorrectly go offline when there are issues with installing a policy on some of the nodes in the cluster.	FW IPS L2FW	116378
In rare cases, the engine might restart due to missing error handling in a state sync routine.	FW	116711
Engines with NetLink configuration might hang under a heavy load when the NetLink status changes.	FW	116756
The Master Engine might restart when a VLAN interface assigned to one Virtual Security Engine is moved to another Virtual Security Engine.	FW IPS L2FW	116835
Anti-spam might not work on engines that have NGF licenses that have been upgraded to version 5.9.	FW	116894
Some log messages do not include the Domain in the **User** field when the default authentication Domain is used.	FW	1085933
Rare IKE messages can cause the ipsecpmd process to generate core files and restart the process. This causes short breaks in IPsec VPN connectivity.	FW	1098060
In VPN Multi-Link setups where some VPN endpoints are inside the configured VPN site, you might see VPN negotiation errors, such as: "IPsec SA responder error: No proposal chosen."	FW	1100479

Installation instructions

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

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

The sgadmin user is reserved for McAfee use on Linux, so it must not exist before SMC is installed for the first time.

Task

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.
- McAfee 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 SMC and McAfee servers 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.

- McAfee 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.

- McAfee 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.

Task

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 McAfee product has a comprehensive set of documentation.

- *McAfee Next Generation Firewall Product Guide*
- McAfee Next Generation Firewall online Help

> By default, the online Help is used from the McAfee 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*

B00