FORCEPOINT

NGFW Security Management Center Appliance

Release Notes

6.2.0

Revision A

Contents

About this release

This document contains important information about this software release for the Forcepoint NGFW Security Management Center Appliance (SMC Appliance).

We strongly recommend that you read the entire document.

The SMC Appliance ships with pre-installed Forcepoint NGFW Security Management Center (SMC) software. The pre-installed SMC includes a Management Server and a Log Server.

Note: The SMC Appliance does not support high-availability for the Management Server or the Log Server.

The SMC Appliance software can also be installed on a virtualization platform. For more information, see the *Forcepoint Next Generation Firewall Installation Guide*.

Compatibility

SMC 6.2 has the following requirements for compatibility and native support.

Note: SMC 6.2 can manage all compatible Forcepoint NGFW engine versions up to and including version 6.2.

Compatible component versions

SMC 6.2 works with the following component versions.

Note: Some versions of Forcepoint NGFW might have reached end-of-life status. We recommend that you use a Long-Term Support version that is still supported. For more information about the Forcepoint NGFW lifecycle policy, see Knowledge Base article 10192.

- Forcepoint™ Next Generation Firewall (Forcepoint NGFW) 6.2
- Stonesoft® Next Generation Firewall by Forcepoint (Stonesoft NGFW) 6.0 and 6.1
- McAfee® Next Generation Firewall (McAfee NGFW) 5.7, 5.8, 5.9, and 5.10
- Stonesoft Security Engine 5.5
- Stonesoft Firewall/VPN Express 5.5
- McAfee® ePolicy Orchestrator® (McAfee ePO™) 5.0.1 and 5.1.1
- McAfee® Enterprise Security Manager (McAfee ESM) 9.2.0 and later (9.1.0 CEF only)

Native support

To use all features of SMC 6.2, Forcepoint NGFW 6.2 is required.

New features

This release of the product includes these new features. For more information and configuration instructions, see the *Forcepoint Next Generation Firewall Product Guide* and the *Forcepoint Next Generation Firewall Installation Guide*.

Forcepoint Advanced Malware Detection

Forcepoint Advanced Malware Detection uses file reputation scans in a sandbox service to detect advanced threats. The Cloud Sandbox analyzes the behavior of files in a restricted operating system environment and returns a reputation score for the files. From the Logs view of the Management Client, you can access an external portal where you can view detailed reports for files that have been analyzed in the Cloud Sandbox. You can also use analysis and reporting tools in the external portal.

Note: Forcepoint Advanced Malware Detection requires a separate license for the Cloud Sandbox service. See Knowledge Base article 12514.

Pending configuration changes shown for NGFW Engines

You can now view configuration changes that you and other administrators have made before the new configurations are transferred to the engines. The pending changes are shown in the Home view and on the selected engine's home page. You can optionally also enforce an approval workflow. When an approval workflow is enforced, administrators with unrestricted permissions must approve all pending changes before the changes can be committed.

New search bar in the Management Client

There is a new search bar in the Management Client header. The search bar is the fastest way to find elements, folders, and actions. You can also access related drill-down actions, and drag and drop elements from the search results list to other views, such as the Policy Editing view or the Routing view for an engine.

Support for Sidewinder Proxies on Virtual NGFW Engines in the Firewall/VPN role

You can now use Sidewinder Proxies (HTTP, SSH, TCP, and UDP) on Virtual NGFW Engines in the Firewall/VPN role. Sidewinder Proxies on Forcepoint NGFW enforce protocol validation and restrict the allowed parameters for each protocol. Sidewinder Proxies are primarily intended for users in high assurance environments, such as government or financial institutions. In environments that limit access to external networks or access between networks with different security requirements, you can use Sidewinder Proxies for data loss protection.

DNS Relay on NGFW Engines in Firewall/VPN role

DNS relay allows NGFW Engines in the Firewall/VPN role to provide DNS services for internal networks. The firewall forwards DNS requests from clients in the internal network to remote DNS servers and temporarily stores the results of the DNS requests in the cache. The firewall can forward DNS requests to different DNS servers depending on the domain in the DNS request. The firewall can also return fixed DNS results for specific hosts or domains, and translate external IP addresses in DNS replies to IP addresses in the internal network.

Improved dynamic multicast routing support on NGFW Engines in Firewall/VPN role

You can now configure protocol-independent multicast (PIM) on NGFW Engines in the Firewall/VPN role in the Management Client. Previously, you could only configure PIM on the engine command line. You can use source-specific multicast (PIM-SSM), sparse mode (PIM-SM), or dense mode (PIM-DM).

Improved logging and diagnostics for SSL VPN Portal

Logging and diagnostics have been improved for the SSL VPN Portal. Log entries are generated when an SSL VPN Portal user starts and ends a session. If diagnostics are enabled for the SSL VPN Portal, log entries are also generated for HTTP or HTTPS transactions. SSL VPN Portal users can see the time of their last logon and the number of failed logon attempts in the status bar of the SSL VPN Portal.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.2.0

Enhancement	Description
NetLink-specific DNS IP addresses	You can now define NetLink-specific DNS IP addresses for static NetLinks. Dynamic NetLinks can automatically learn DNS IP addresses.

Enhancement	Description
Improved configuration of User Responses	User Responses are now easier to configure. The new message response allows you to quickly create simple messages without using HTML markup. You can also use variables in User Responses to provide connection-specific information to the end users.
Improvements to Home view and Management Client look-and-feel	Several small enhancements have been made to the Home view in the Management Client. The look-and-feel of the Management Client has also been improved. For example, in the Home view, the layout of the panes changes dynamically, and you can now access relevant drill-down actions when you place the cursor over status cards for NGFW Engines and VPN elements.
Improvements in the Logs view	You can now save your column selections and layout in the Logs view.
Improvements in log forwarding performance	Log forwarding performance has been improved on the Log Server.
Improvements in Overviews	The maximum tracking period is now one month instead of one day in Overviews.
Automatic licensing on first-time installations	When you install the SMC for the first time, it now sends the proof-of-license codes to the Forcepoint License Center, and it generates and installs new licenses automatically by default.

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	Issue number
If a more recent dynamic update package than the one included in the SMC installation files is active when you upgrade the SMC, the following message is shown during the upgrade: "Import of Initial Update Package Failed: Automatic update package import or activation failed. Please import and activate the update package in the Management Client." When you upgrade to a new maintenance version of the same major version, it is not necessary to activate the dynamic update package that is included in the SMC installation files. When you upgrade to a new major version, you must activate the dynamic update package that is included in the SMC installation files. For more information, see Knowledge Base article 12381.	SMC-614
When the Source cell of an Access rule includes a firewall element that has a dynamic IP address, the whole rule is ignored. The following kind of warning is shown during policy validation: "The IPv4 Access rule @X.X is ignored. Source must not contain an element with a dynamic IP address."	SMC-655
When you use the Web Start Management Client on Mac OS X, you cannot select status cards in the Home view to open the home page for an element.	SMC-908
When you create a rule from a log entry for a file that was discarded according to the File Filtering Policy, the rule is incorrectly created in the Inspection Policy.	SMC-1112

Description	Issue number
The Expression Properties dialog box might not display all fields on small monitors. The expression at the bottom of the dialog box might be hidden.	SMC-1173
The duplicate element warning is not shown when the name of a new element is a non-case-sensitive match for the name of an existing element. For example, if the name of the new element starts with a capital letter and the name of the existing element is all lower case, the warning is not shown.	SMC-1430
You cannot add Users from domains other than the Default LDAP Domain to a rule using the Edit Source or Edit Destination right-click options.	SMC-1739
The following validation warning is shown even if anti-malware is not enabled in the engine properties and there are no Access rules that enable file filtering: "Anti-Malware is enabled in rule @260036.0, but no Anti-Malware Add-Ons are enabled in the properties of Firewall Cluster <name>. General Checks Anti-Malware Scan is enabled in rule @260036.0, but the GTI usage has not been authorized in the Global System Properties. Anti-Malware cannot be used." For more information, see Knowledge Base article 10202.	SMC-1812
The number of active alerts shown on the status cards for NGFW Engines in the Home view might not be refreshed.	SMC-2406
If the value of the Severity field of an Exception rule in an Inspection Policy is Information or a Severity Range that includes the Information level, policy installation fails. The following message is shown during policy installation: "creating sg_inspection configuration failed".	SMC-2697
When you use administrative Domains, it might not be possible to create a user in the InternalDomain LDAP domain in any Domain other than the Shared Domain. The following type of message is shown: "Invalid Parameter: DB key missing".	SMC-3020
When viewing a report, the "Show Records" option might be missing from the right-click menu in a report section if the data is based on log entries.	SMC-3149
In rare cases in environments with multiple Management Servers, an active Management Server might be shown in the Isolated state in the Control Management Servers dialog box. Automatic replication fails for the Management Server in the Isolated state, but manual replication is successful.	SMC-3161
Setting the channel to Automatic on a Wireless Interface is only supported on engine versions 6.0 or higher. Policy validation does not prevent this configuration on older engine versions, but policy installation fails because the configuration is not supported.	SMC-3693
You can add only one IP address to each SSID Interface of a Wireless Interface.	SMC-3772
Creating new Virtual NGFW Engines using the SMC API fails.	SMC-4155

Installation instructions

Use these high-level steps to install the SMC Appliance.

For detailed information about installing the SMC Appliance and the NGFW Engines, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at https://support.forcepoint.com.

Steps

1) Turn on the SMC Appliance.

2) Select the keyboard layout for accessing the SMC Appliance on the command line.

3) Accept the EULA.

4) Enter the account name and password.
   For credential requirements, see the *Forcepoint Next Generation Firewall Installation Guide*.

5) Make your security selections.

6) Complete the network interface and network setup fields.

7) Enter a host name for the Management Server.

8) Select the time zone.

9) (Optional) Configure NTP settings.

10) After the SMC Appliance has restarted, install the Management Client.
    You can use Java Webstart or install the Management Client from a file to allow remote access to the SMC. Java Web Start is enabled by default on the Management Server that is pre-installed on the SMC Appliance.

11) Create the NGFW Engines elements, then install and configure the NGFW Engines.

Install SMC Appliance patches

The SMC Appliance patches can include improvements and enhancements to the SMC software, the operating system, or the SMC Appliance hardware.

The SMC Appliance patch (SAP) format is specific to the SMC Appliance. The SAP numbering is appended to the version number (for example, 6.2.0P01).

SMC Appliance maintenance patches are managed on the command line. If you do not have physical access to the SMC Appliance, use SSH to access the SMC Appliance remotely. For more details, see the *Forcepoint Next Generation Firewall Product Guide*.

Note: You must have superuser administrator permissions on the SMC Appliance to manage SMC Appliance patches. Use sudo if you need elevated privileges. For a list of available sudo commands, enter `sudo -l` on the command line.

Steps

1) Log on to the SMC Appliance.

2) Enter `sudo ambr-query` and press **Enter** to check for available patches.

3) Enter `sudo ambr-load <patch>` and press **Enter** to load the patch on the SMC Appliance.

4) Enter `sudo ambr-install <patch>` and press **Enter** to install the patch on the SMC Appliance.

Known issues

For a list of known issues in this product release, see Knowledge Base article 12495.

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.

- *Forcepoint Next Generation Firewall Product Guide*
- Forcepoint 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.

- *Forcepoint Next Generation Firewall Installation Guide*

Other available documents include:

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