About this release

This document contains important information about this release of Forcepoint Next Generation Firewall (Forcepoint NGFW).

We strongly recommend that you read the entire document.

Lifecycle model

This release of Forcepoint NGFW is a Long-Term Support (LTS) version.

We recommend using the most recent Long-Term Support (LTS) version if you do not need any features from a later Feature Stream version.

For more information about the Forcepoint NGFW lifecycle policy, see Knowledge Base article 10192.
System requirements

To use this product, your system must meet these basic hardware and software requirements.

Forcepoint NGFW appliances

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

Note: Some features in this release are not available for all appliance models. See Knowledge Base article 9743 for up-to-date appliance-specific software compatibility information.

The following table shows whether you can use an appliance model in the Firewall/VPN (FW), IPS, or Layer 2 Firewall (L2FW) role.

<table>
<thead>
<tr>
<th>Appliance model</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>320X (MIL-320)</td>
<td>FW</td>
</tr>
<tr>
<td>FWL321</td>
<td>FW</td>
</tr>
<tr>
<td>NGF321</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>FWL325</td>
<td>FW</td>
</tr>
<tr>
<td>NGF325</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>110</td>
<td>FW</td>
</tr>
<tr>
<td>115</td>
<td>FW</td>
</tr>
<tr>
<td>1035</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>1065</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>1101</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>1105</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>1401</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>1402</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>2101</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>2105</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>3202</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>3206</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>3207</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>3301</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>3305</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>5206</td>
<td>FW, IPS, L2FW</td>
</tr>
<tr>
<td>6205</td>
<td>FW, IPS, L2FW</td>
</tr>
</tbody>
</table>
Sidewinder S-series appliances

These Sidewinder appliance models can be re-imaged to run Forcepoint NGFW software.

<table>
<thead>
<tr>
<th>Appliance model</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-1104</td>
<td>FW</td>
</tr>
<tr>
<td>S-2008</td>
<td>FW</td>
</tr>
<tr>
<td>S-3008</td>
<td>FW</td>
</tr>
<tr>
<td>S-4016</td>
<td>FW</td>
</tr>
<tr>
<td>S-5032</td>
<td>FW</td>
</tr>
<tr>
<td>S-6032</td>
<td>FW</td>
</tr>
</tbody>
</table>

Certified Intel platforms

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

The tested platforms can be found at https://support.forcepoint.com under the Forcepoint Next Generation Firewall product.

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

Basic hardware requirements

You can install Forcepoint 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.](image)

- IDE hard disk and DVD drive

  ![Note: IDE RAID controllers are not supported.](image)

- 4 GB RAM minimum
- 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 NGFW Engine requirements

Master NGFW Engines have specific hardware requirements.

- Each Master NGFW Engine must run on a separate physical device. For more details, see the Forcepoint Next Generation Firewall Installation Guide.
- All Virtual NGFW Engines hosted by a Master NGFW Engine or Master NGFW Engine cluster must have the same role and the same Failure Mode (fail-open or fail-close).
- Master NGFW Engines can allocate VLANs or interfaces to Virtual NGFW 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 NGFW Engine cluster in standby mode.
- Cabling requirements for Master NGFW 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 Forcepoint Next Generation Firewall Installation Guide.

Virtual appliance node requirements

You can install Forcepoint 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 6.0 and 6.5
  - KVM (KVM is tested as shipped with Red Hat Enterprise Linux Server 7.1 and 7.2)
  - Microsoft Hyper-V on Windows Server 2012 or Windows Server 2016 (Firewall/VPN role only)
    An Intel 64-bit processor is required.
- 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 Forcepoint 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 Forcepoint NGFW is run as a virtual appliance node in the IPS or Layer 2 Firewall role, clustering is not supported.
Build version

Forcepoint NGFW 6.4.0 build version is 20027.

Product binary checksums

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

- sg_engine_6.4.0.20027_x86-64-small.iso

  SHA1SUM: f56ad497a6287b229990f9bd6fc6333c9b3b891d
  SHA256SUM: 1fe13f638c7901e9a13676b1599773fc6b8d2bb3e838289a357746254bc97973
  SHA512SUM: 8eece2f6fc7b5e89d3e9cd4d7b162a120954e76e89da1d776f014c5a499c450f01c8856a1d294d36081ea73cf923f73e9e5f04b928fc4f27063011b18

- sg_engine_6.4.0.20027_x86-64-small.zip

  SHA1SUM: a78792c86f6e7067b62567b9d21f3c39ff8
  SHA256SUM: 5729a2744e6ba0da3f11658c0a590ad16a16bb3d79630853121470b004ed4
  SHA512SUM: 31cebd8349c65d5a1dd1db10f9968b637763d0061e611d0a24360cd8bc32f01b486d10ed06ed655a9032f85e1a2a55463c2aa3afdc6778e15cd246942381c

Compatibility

Forcepoint NGFW 6.4 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.4 or higher
- Dynamic Update 1041 or higher
- Stonesoft® VPN Client for Windows 6.0.0 or higher
- Stonesoft® VPN Client for Mac OS X 2.0.0 or higher
- Stonesoft® VPN Client for Android 2.0.0 or higher
- Server Pool Monitoring Agent 4.0.0 or higher
- Forcepoint Endpoint Context Agent (ECA) 1.1.0 or higher
- Forcepoint User ID Service 1.1.0 or higher
- McAfee® Logon Collector 2.2 and 3.0
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.

Redirection of HTTP and HTTPS traffic to a proxy

The NGFW Engine can now transparently redirect HTTP and HTTPS traffic to a proxy. The proxy can be on-premises or a cloud-based service, such as the Forcepoint Web Security Cloud service. The traffic does not have to be redirected through a policy-based VPN.

Improved integration of external NTP servers

You can now use external NTP servers to provide time synchronization for both the SMC Appliance and NGFW Engines. External NTP servers were previously supported only for the SMC Appliance. You can use the same NTP servers for the SMC Appliance and the NGFW Engines.

SNMP Agent enhancements

You can now use SNMP Agents when you configure SNMP for the SMC Appliance. SNMP Agents were already supported for NGFW Engines in previous versions.

You can now specify the SNMP engine ID for each NGFW Engine and for the SMC Appliance. The SNMP engine ID is a unique identifier that the SNMP Agent uses to for the NGFW Engine or the SMC Appliance.

SNMP Agents now support IPv6 addresses.

Note: If you configured SNMP for the SMC Appliance before upgrading to version 6.4.0, you must configure SNMP again after upgrading to version 6.4.0 or higher.
## Enhancements

This release of the product includes these enhancements.

### Enhancements in Forcepoint NGFW version 6.4.0

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
</table>
| Improved integration of external LDAP servers and Active Directory servers | The integration of external LDAP servers and Active Directory servers with Forcepoint NGFW has been improved.  
- Support for the LDAPS and Start TLS protocols for securing the LDAP connection has been improved. When LDAPS or Start TLS is enabled for an LDAP Server or Active Directory Server, you can now select a TLS Profile and TLS Server Identity for the LDAP Server.  
- A new Authentication Method element for LDAP Authentication has been added. When LDAP Authentication is configured for a user, the user’s password is checked against the user’s credentials in the LDAP server that is used for user storage. LDAP Authentication can be used with the following existing features: IPsec and SSL tunnels in mobile VPNs, the SSL VPN Portal, and browser-based user authentication. |
<p>| Improvements in browser-based user authentication | Browser-based user authentication now supports certificate-based authentication. Users can authenticate using a certificate file, or a certificate stored on a smart card, such as a Common Access Card (CAC). |
| Other authentication enhancements | The Require Authorization and Timeout for Client IP Authorization options have been removed from Authentication options for Access rules. Authorization is automatically required when you add User and Authentication Method elements to the Authentication cell. The Authentication Time-Out option in the Add-Ons &gt; User Authentication branch of the Engine Editor replaces the Timeout for Client IP Authorization option. |
| Improvements in application detection | Because Access rules for application detection match traffic based on the payload of connections, the same connection can potentially match more than one rule based on the first SYN packet of the connection. Connection handling such as the use of VPNs, NAT, SSM Proxies, and TCP MSS enforcement is applied according to the initial match. When the final match is different from the initial match in a way that changes connection handling, the connection is dropped. In these cases, a log message that indicates a conflict between rules is generated. Note: Due to changes in application detection, policies that use Network Applications, URL Categories, or URL Lists in the Access rules might work differently after upgrading to NGFW 6.4. Some traffic that was previously allowed might be discarded. After upgrading to NGFW 6.4 or higher, verify that your policies work as expected. For more information, see Knowledge Base article 15411. |</p>
<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Network Application elements of the Cloud Services type</td>
<td>New Network Application elements of the Cloud Services type have been added to the SMC from the Forcepoint cloud access security broker (CASB) service catalog. Including the previous Network Application elements of the Web Applications and Protocols types, there are now over 7000 Network Applications available.</td>
</tr>
<tr>
<td>Duplicate IPv6 address detection for Layer 3 Physical Interfaces</td>
<td>An option for detecting duplicate IPv6 addresses has been added to the Layer 3 Physical Interface properties for NGFW Engines.</td>
</tr>
<tr>
<td>Bootloader password for NGFW Engines</td>
<td>During the initial configuration, you can now specify a bootloader password for the NGFW Engine. To edit the options that appear in the bootloader, you must enter the bootloader password.</td>
</tr>
<tr>
<td>Layer 2 Physical Interfaces on Virtual Firewalls and Master Engines that host Virtual Firewalls</td>
<td>You can now configure Layer 2 Physical Interfaces on Virtual Firewalls and Master Engines that host Virtual Firewalls.</td>
</tr>
<tr>
<td>Easier deployment of NGFW Engines in Microsoft Azure</td>
<td>You can now deploy NGFW Engines from the Microsoft Azure cloud environment without first creating the NGFW Engine element in the Management Client. You deploy the NGFW Engines from the cloud environment, and you can monitor the NGFW Engines in the Management Client.</td>
</tr>
<tr>
<td>Auto-scaling in Microsoft Azure</td>
<td>Support for auto-scaling for NGFW Engines that are deployed in Azure has been added. When the scaling feature is used, additional NGFW Engine instances are automatically created and removed, depending on traffic load. You can monitor the NGFW Engine instances in the Management Client.</td>
</tr>
<tr>
<td>Cloud Sandbox analysis information in the external portal</td>
<td>You can now view analysis information in the external portal for the cloud sandbox. You must define a user name for the cloud service in the Management Client to be able to view the analysis information in the external portal.</td>
</tr>
<tr>
<td>Auto-discovery for ECA clients</td>
<td>The NGFW Engine can now advertise its contact address to ECA clients. If the contact address of the NGFW Engine changes, or a new NGFW Engine is added to the network, the ECA clients are still able to connect to the NGFW Engine.</td>
</tr>
<tr>
<td>Monitoring of Forcepoint User ID Service</td>
<td>You can now enable monitoring for the Forcepoint User ID Service. You can also configure that the Forcepoint User ID Service sends log data to the SMC.</td>
</tr>
<tr>
<td>License reporting tool</td>
<td>There is a new tool for MSSP customers that exports all data related to licenses and NGFW Engines to a CSV file.</td>
</tr>
</tbody>
</table>
Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in a previous release, see the Release Notes for the specific release.

<table>
<thead>
<tr>
<th>Description</th>
<th>Role</th>
<th>Issue number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access rules that discard traffic based on detection of a Network Application might incorrectly block other traffic that matches a later rule that should forward traffic to a VPN or for processing by a SSM proxy.</td>
<td>FW</td>
<td>NGFW-2046</td>
</tr>
</tbody>
</table>

Installation instructions

Use these high-level steps to install SMC and the Forcepoint NGFW engines.
For detailed information, see the Forcepoint 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.

Note: If you install the SMC on Windows 10 and Windows Defender is enabled, it might take a long time to activate a dynamic update package. For more information, see Knowledge Base article 14055.

Steps

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 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.

**Note:** Upgrading to version 6.4 is only supported from version 6.3 or higher. If you have a lower version, first upgrade to version 6.3.

**Note:** Starting from Forcepoint NGFW version 6.4, the McAfee Advanced Threat Defense feature is no longer supported. We recommend that you use Forcepoint Advanced Malware Detection instead.

- Forcepoint NGFW version 6.4 requires an updated license. 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 DVD and follow the instructions. For detailed instructions, see the Forcepoint Next Generation Firewall Installation Guide.
- If you have customized the sshd_config file in the /data/config/ssh directory, you might need to manually update the configuration file after upgrading the engine to Forcepoint NGFW version 6.4. See Knowledge Base article 10461.

**Known issues**

For a list of known issues in this product release, see Knowledge Base article 15420.

**Known limitations**

This release of the product includes these known limitations.

<table>
<thead>
<tr>
<th>Limitation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspection in asymmetrically routed networks</td>
<td>In asymmetrically routed networks, using the stream-modifying features (TLS Inspection, URL filtering, and file filtering) can make connections stall.</td>
</tr>
<tr>
<td>Inline Interface disconnect mode in the IPS role</td>
<td>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.</td>
</tr>
</tbody>
</table>

For information about feature-specific limitations, see the Forcepoint Next Generation Firewall Product Guide.
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*