FORCEPOINT

Next Generation Firewall

Release Notes

6.3.2

Revision A

Contents

- About this release on page 2
- Lifecycle model on page 2
- System requirements on page 3
- Build version on page 6
- Compatibility on page 6
- New features on page 7
- Enhancements on page 8
- Resolved issues on page 10
- Installation instructions on page 14
- Known issues on page 16
- Find product documentation on page 16

About this release

This document contains important information about this release of Forcepoint™ Next Generation Firewall (Forcepoint NGFW), formerly known as Stonesoft® Next Generation Firewall by Forcepoint (Stonesoft 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

Make sure that you 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.

Appliance model	Roles
FW-315	FW
320X (MIL-320)	FW
IPS-1205	IPS, L2FW
FWL321	FW
NGF321	FW, IPS, L2FW
FWL325	FW
NGF325	FW, IPS, L2FW
110	FW
115	FW
1035	FW, IPS, L2FW
1065	FW, IPS, L2FW
1101	FW, IPS, L2FW
1105	FW, IPS, L2FW
1301	FW, IPS, L2FW
1302	FW, IPS, L2FW
1401	FW, IPS, L2FW
1402	FW, IPS, L2FW
2101	FW, IPS, L2FW
2105	FW, IPS, L2FW
3201	FW, IPS, L2FW
3202	FW, IPS, L2FW
3205	FW, IPS, L2FW

Appliance model	Roles
3206	FW, IPS, L2FW
3207	FW, IPS, L2FW
3301	FW, IPS, L2FW
3305	FW, IPS, L2FW
5201	FW, IPS, L2FW
5205	FW, IPS, L2FW
5206	FW, IPS, L2FW
6205	FW, IPS, L2FW

Sidewinder S-series appliances

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

Appliance model	Roles
S-1104	FW
S-2008	FW
S-3008	FW
S-4016	FW
S-5032	FW
S-6032	FW

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.

- IDE hard disk and DVD drive

  Note: IDE RAID controllers are not supported.

- 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 6.3.2 build version is 19110.

Product binary checksums

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

- sg_engine_6.3.2.19110_x86-64-small.iso

```
SHA1SUM:
97880461bcb2ccc42df72f7428ce7e6bfb63b1ed

SHA256SUM:
57fb3d43b9b4a93f218c90d9d708b7a171474bedc8cdf6920052c503451c2fdd

SHA512SUM:
e8a1f8f0d6ebb6982322d43a2911bb00
bbd241e26cb677885fa04094012c097d
aa33d1a000dae776476648188a877273
ba53394e42f5f6e780c389279f0c1d81
```

- sg_engine_6.3.2.19110_x86-64-small.zip

```
SHA1SUM:
7b8e1eb22f0378b412c239409bcd568113da416c

SHA256SUM:
051467f0a05be69e48c619e268c9eec54ec4a13f3c5aa2294c26d1e466c0d720

SHA512SUM:
6dc67eb861d74ff4d89a852c4e6dc730
3de76e7273df82e707ed2fe4817dd0fe
953fa89cd4e56ba9826fdf205b1febc4
2fa187aed3c4d773c60bd4d5e4a6a1df
```

Compatibility

Forcepoint NGFW 6.3 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.3 or later
- Dynamic Update 988 or later
- Stonesoft® VPN Client for Windows 6.0.0 or later
- Stonesoft® VPN Client for Mac OS X 2.0.0 or later
- Stonesoft® VPN Client for Android 2.0.0 or later
- Server Pool Monitoring Agent 4.0.0 or later

- Forcepoint Endpoint Context Agent (ECA) 1.1.0
- Forcepoint User ID Service 1.1.0
- McAfee® Logon Collector 2.2 and 3.0
- McAfee® Advanced Threat Defense 4.0

Note: Forcepoint NGFW 6.3 is the last major version that supports McAfee Logon Collector and McAfee Advanced Threat Defense.

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*.

Support for Forcepoint Endpoint Context Agent

Support for Forcepoint Endpoint Context Agent (ECA) allows you to use endpoint information in the Forcepoint NGFW policy to control access, identify users, and log their actions. ECA is a Windows client application that provides endpoint information to the NGFW Engine. ECA is a replacement for McAfee Endpoint Intelligence Agent (McAfee EIA).

CAUTION: If McAfee Endpoint Intelligence Agent (McAfee EIA) is configured on the NGFW Engine when you upgrade to version 6.3 or later, the NGFW Engine node is returned to the initial configuration state and stops processing traffic. You must remove the McAfee Endpoint Intelligence Agent (McAfee EIA) configuration and refresh the policy before you upgrade to version 6.3 or later. For more information, see Knowledge Base article 14093.

Multi-Layer Deployment for NGFW Engines in the Firewall/VPN role

Multi-layer deployment is now supported for NGFW Engines in the Firewall/VPN role. In multi-layer deployment, NGFW Engines in the Firewall/VPN role have both layer 2 physical interfaces and layer 3 physical interfaces. The same NGFW Engine can now provide the features of the Firewall/VPN role, as well as the inspection features of the IPS and Layer 2 Firewall roles.

Route-based VPN improvements

The user interface for configuring a route-based VPN has been improved. Instead of configuring a single Route-Based VPN element, you can create individual Route-Based VPN Tunnel elements. The route-based VPN tunnels can be used in Administrative Domains other than the Shared Domain.

Improvements in Forcepoint Advanced Malware Detection

In addition to the cloud sandbox, Forcepoint Advanced Malware Detection now also supports on-premises local sandboxes. Other improvements include the following:

- The NGFW Engine can now delay file transfers until the results of the sandbox scan are received.
- The NGFW Engine now separately requests a file reputation for each file in .zip archives.
- The reporting tools in the external portal have been improved, and it is easier to access reports in the external portal from the Management Client.

NGFW on Azure and Hyper-V

You can now deploy NGFW Engines in the Microsoft Azure cloud to provide VPN connectivity, access control, and inspection for services in the Microsoft Azure cloud. The Microsoft Hyper-V virtualization platform on Windows 2012 and 2016 servers is now also supported for NGFW deployment on a virtualization platform in a private cloud. Only NGFW Engines in the Firewall/VPN role are supported in the Microsoft Azure cloud and on the Microsoft Hyper-V virtualization platform.

Support for Forcepoint User ID Service

Forcepoint User ID Service collects information about users, groups, and IP addresses from Windows Active Directory (AD) servers and AD domains. You can use the information from the Forcepoint User ID Service in the Forcepoint NGFW policy to identify users and control access.

Support for HTTPS in Sidewinder HTTP Proxy

The Sidewinder HTTP Proxy can now provide decryption, inspection, protocol validation, certificate validation, and certificate revocation checking for the HTTPS protocol.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 6.3.0

Enhancement	Description
Rate limit per Virtual NGFW Engine for traffic from the Master NGFW Engine	You can now set a rate limit per Virtual NGFW Engine for traffic from the Master NGFW Engine to the Virtual NGFW Engine. When the limit is set, a single Virtual NGFW Engine that is under very heavy load cannot disrupt the operation of the other Virtual NGFW Engines that are hosted by the Master NGFW Engine.

Enhancement	Description
Dedicated control plane operation	You can now dedicate a specified number of CPUs to control plane operations. Even under very heavy loads, you can continue to manage NGFW Engines and refresh policies, and the status of the NGFW Engines remains green in the Home view.
Changes related to certificates	The NGFW Engine can now validate certificates and check the certificate revocation status for features that have certificate validation and certificate revocation checks enabled, such as features that use a TLS Profile in the configuration. Except for VPN certificates, most elements related to certificates are now found in the **Administration** > **Certificates** branch of the **Configuration** view. There is no longer a separate Pending Certificate Request element. Certificate requests are now created as TLS Credentials elements. The state of the TLS Credentials element indicates whether is it a signed certificate or a certificate request.
Limit for half-open TCP connections	As part of the SYN flood protection feature, you can now set a limit for the number of half-open TCP connections. When the limit is reached, SYN flood protection is enabled.
Improvements to SSM architecture	Improvements to SSM integration remove some previous limitations on inspection when Sidewinder Proxies are used. These former limitations include matching traffic based on Network Applications, file filtering, and URL filtering. New Combined Protocol elements allow you to apply a standard Protocol element and a Sidewinder Proxy Protocol element to the same traffic.
New commands for managing NGFW Engines and NGFW appliances	It is now possible to power off an NGFW Engine remotely through the Management Client. In addition, you can now also reset an NGFW appliance to factory settings through the Management Client. To increase security, you can set how many times you want the stored data on the file system of the NGFW appliance to be overwritten.
Task for validating policies	There is a new task for validating policies. The Validate Policy task allows you to validate the policy installed on NGFW Engines or Master NGFW Engines or the Alert Policy installed in an administrative Domain. You can run the Validate Policy task either manually or according to a schedule.
SYN rate limits support IPv6 connections	SYN rate limits now also support IPv6 connections.
Log rate and spooled log information available in engine status monitoring	In the engine status monitoring, you can now see the log rate and the times at which logs have been spooled on the engine.
Improved dynamic routing monitoring	Changes in the OSPF and BGP neighborhood trigger alerts that are visible in the Logs view of the Management Client. Information about route changes is also included in logs.
Improved inspection for flash files	The NGFW Engine now supports the inspection of flash files, allowing it to detect potential security threats in flash files.
Faster rule matching for dynamic elements	Rule matching for rules that contain DNS names, users, and user groups is now faster. This improvement is especially useful when the policy uses a large number of these elements.

Enhancements in Forcepoint NGFW version 6.3.2

Enhancement	Description
Dynamic routing throughput improved	The throughput of dynamically routed packets has improved.
SNI in TLS communications for the SSL VPN Portal	The SSL VPN Portal now uses the server name indication (SNI) in TLS communications between the NGFW Engine and web resources.
IGMP-based multicast forwarding enhancement	When an NGFW Engine is used as an IGMP proxy for multicast forwarding, the number of supported multicast groups has increased.

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
On Virtual Firewalls, some static routes might be removed if you move networks and routing configurations from one interface to another, or if you create a new Aggregated Link interface.	FW	NGFW-1275
Multicast DNS connections are not cleared from the connection table when connections are processed by a DNS proxy.	FW	NGFW-6671
Access rules that match based on the source VPN might match non-VPN traffic if the source, destination, and service match the connection, and deep inspection, application matching, or application logging is enabled.	FW	NGFW-7092
Logs of the type Connection_Allowed do not show the destination interface, destination VLAN, or destination zone if the connection that generated the log entry was inspected.	FW, IPS, L2FW	NGFW-7142
If SNMP is configured, it does not work with interfaces that have PPP enabled.	FW	NGFW-7223
When the NGFW Engine processes a large number of SIP connections and NAT is used, the inspection process might restart.	FW	NGFW-7270
If an NGFW Engine is selected in the Home view of the Management Client, the memory consumption of the selected node might start to increase while the Home view remains open. The memory is released when you close the Management Client.	FW, IPS, L2FW	NGFW-7303
The connection between the Endpoint Context Agent (ECA) client and the NGFW Engine fails if the ECA client uses a certificate created by Microsoft Active Directory Certificate Services (AD CS).	FW, IPS, L2FW	NGFW-7525
When the NGFW Engine connects to a Forcepoint User ID Service server, the source IP address is selected based on routing, and does not adhere to the "Source for Authentication Requests" interface option.	FW, IPS, L2FW	NGFW-7540
Policy installation or refresh might not finish successfully.	FW, IPS, L2FW	NGFW-7558
The redirection link on the logon page for browser-based user authentication does not work if the URI includes a port.	FW	NGFW-7641

Description	Role	Issue number
In rare cases, the inspection process might restart if inspection is used. The NGFW Engine might need to be restarted.	FW, IPS, L2FW	NGFW-7666
If multiple users are logged on to the same endpoint computer, the logs related to Endpoint Context Agent (ECA) might show the wrong user.	FW, IPS, L2FW	NGFW-7693
The inspection process in the NGFW Engine might restart if there are a large number of new connections from Endpoint Context Agent (ECA) clients.	FW, IPS, L2FW	NGFW-7725
Connections reported by Endpoint Context Agent (ECA) clients to the NGFW Engine might not match the users or groups configured in the Access rules, and in the logs, the external LDAP Domain that is configured in the Management Client is shown in the User field, instead of the real domain.	FW, IPS, L2FW	NGFW-7743
Browser-based user authentication might not work correctly when dynamic routing is configured for the same NGFW Engine. This issue prevents the policy from being successfully refreshed on the NGFW Engine, and prevents the use of browser-based user authentication.	FW	NGFW-7746
The proxy process might restart if a proxied connection is inspected and the connection is matched against an Access rule that refers to Endpoint Context Agent (ECA) components or if the logging of endpoint information is enforced.	FW	NGFW-7763
When Forcepoint Endpoint Context Agent or McAfee Endpoint Intelligence Agent is integrated with NGFW, memory consumption on the NGFW Engine can increase significantly.	FW, IPS, L2FW	NGFW-7819
When processing certain types of traffic, the HTTP proxy process might restart.	FW	NGFW-7839
If the NGFW Engine decrypts TLS traffic or there is a User Response to an inspected connection, and connection initiation packets are then re-transmitted, the connection might fail.	FW, IPS, L2FW	NGFW-7871
When you refresh the policy on the Master NGFW Engine, but not on the Virtual Firewall, the authentication page for browser-based user authentication might not load completely, or user authentication might time out soon after a user authenticates if session handling is enabled on the User Authentication branch of the Engine Editor.	FW	NGFW-7875
If both an HTTP and an HTTPS port are defined, and "Always use HTTPS" is selected on the User Authentication branch of the Engine Editor, connections to the HTTP port are forwarded to the listening IP address for the HTTPS port even if the original connections use a DNS name. This issue can cause HTTPS connections to fail with a certificate error.	FW	NGFW-7982
When connections that are inspected produce an excessive number of log entries, the memory consumption of the NGFW Engine might increase substantially.	FW, IPS, L2FW	NGFW-7990
When you create a Virtual NGFW Engine for a Master NGFW Engine that has an aggregated interface that has VLANs allocated to the Master NGFW Engine, when the policy with the Virtual NGFW Engine configuration is installed, the Link Status engine test reports a failure.	FW	NGFW-8016

Description	Role	Issue number
DHCP requests sent by the NGFW Engine for mobile VPN clients might not be accepted by some DHCP servers.	FW	NGFW-8044
If the Endpoint Context Agent (ECA) configuration, for example, the source or destination networks, is changed in the Management Client, the NGFW Engines might provide the old version of the configuration to the ECA clients on the endpoints.	FW, IPS, L2FW	NGFW-8053
The NGFW Engine might match traffic against Access rules and create logs based on Endpoint Context Agent (ECA) metadata from modified executables. Executable properties that might be modified, are the signer name, product name, product version, or file name, for example.	FW, IPS, L2FW	NGFW-8061
If a VPN client connection is not correctly terminated, such as when there are intermittent connectivity issues, and cluster load balancing allocates the new connection to another node in the cluster, more than one node in the cluster might have an active DHCP lease for the same IP address. This issue can prevent some connections.	FW	NGFW-8066
If DHCP relay is configured on multiple interfaces, including the interface through which the DHCP server is reached, the NGFW Engine might stop forwarding DHCP offers to clients even though the NGFW Engine receives DHCP offers.	FW	NGFW-8092
When a Master NGFW Engine node goes offline or online, or a Master NGFW Engine node restarts, the dynamic routing process might not start correctly on the Master NGFW Engine.	FW	NGFW-8122
The Endpoint Context Agent (ECA) client reports traffic from locally-created users, even though this user information is not used for logging and matching in Access rules. Only user information from Active Directory domains is used for logging and matching in Access rules.	FW, IPS, L2FW	NGFW-8125
When you delete a Virtual Firewall that has dynamic routing configured, the dynamic routing configuration is not deleted from the Master NGFW Engine. If you create a new Virtual Firewall that has uses same Virtual Resource, the new Virtual Firewall might start with the dynamic routing configuration from the deleted Virtual Firewall.	FW	NGFW-8163
When you move a Virtual NGFW Engine to a different Master NGFW Engine node, IPv6 routes might not be propagated from the BGP configuration to the routing table for the Virtual NGFW Engine. Routes might be visible when you use VTYSH on the command line, but they do not appear in the Virtual NGFW Engine properties in the Management Client.	FW	NGFW-8192
When browser-based user authentication is used in a recently-created Virtual NGFW Engine, the logon page might not load properly until the NGFW Engine has been restarted.	FW	NGFW-8202
SSL VPN Portal configurations cannot be installed on Virtual NGFW Engines.	FW	NGFW-8203
When you remove a Virtual Firewall that has a route-based VPN tunnel of the GRE tunnel type, interface tests fail and only one Master NGFW Engine node stays online.	FW	NGFW-8228
The dynamic routing suite has been updated to address CVE-2017-16227.	FW	NGFW-8270

Description	Role	Issue number
When the NGFW Engine requests a virtual IP address for a VPN client from a DHCP server, user and user group information might not be included in the request.	FW	NGFW-8340
Two-factor authentication using the SSL VPN Portal does not work.	FW	NGFW-8375
If a session initiation protocol (SIP) connection is processed by a SIP Protocol Agent, and a SIP call is not answered within 30 seconds, the call might end prematurely.	FW, IPS, L2FW	NGFW-8442
When you change the duplex settings using sg-reconfigure on the NGFW Engine command line, the change is not applied. The NGFW Engine uses the "auto" duplex setting.	FW, IPS, L2FW	NGFW-8527
When an HTTP Protocol Agent has URL logging enabled, but the Access rule does not have deep inspection enabled, the URL is not logged.	FW, IPS, L2FW	NGFW-8537
When end users access an SSL VPN Portal Service using the direct URL of the service instead of logging on to the SSL VPN Portal, the users might not be redirected to the service after they authenticate.	FW	NGFW-8543
If you select the "Delay file transfer until the analysis results are received" option for a rule in the File Filtering Policy and it takes a long time to receive the analysis results from the Forcepoint Advanced Malware Detection sandbox server, the inspection process might restart.	FW, IPS, L2FW	NGFW-8559
Refreshing the policy on a Virtual NGFW Engine that has active VPN connections might cause the Master NGFW Engine and its hosted Virtual NGFW Engines to stop processing traffic. You must restart the Master NGFW Engine to start processing traffic again.	FW	NGFW-8680
You cannot use the NGFW Initial Configuration Wizard (sg-reconfigure) in a web browser with 2100 series NGFW appliances.	FW, IPS, L2FW	NGFW-8683
When the NGFW Engine uses a legacy firewall-only license that does not include full inspection, inspection of the protocols that are allowed by the license might not work. Legacy firewall-only licenses allow the inspection of the following protocols: HTTP, HTTPS, DNS, SIP, IMAP, POP3, and SMTP.	FW	NGFW-8717
The policy rollback feature that safeguards the management connection might not be activated if the management interface uses PPP to get an IP address and refreshing the policy causes PPP negotiations to fail.	FW	NGFW-8730
If you change the AS Path, Community, or Extended Community settings in a Route Map element, the changes might not be applied to the dynamic routing configuration that is running on the firewall.	FW	NGFW-8766
TLS decryption might not work for some connections. As a result, the connections fail. If category-based URL filtering is also applied to the decrypted connections, those connections fail.	FW, IPS, L2FW	NGFW-8769
IPsec tunnels through a standby endpoint might be negotiated unnecessarily.	FW	NGFW-8774
In a route-based VPN tunnel which is of the type GRE, IP-IP, or SIT, traffic might stop being processed after the policy is refreshed.	FW	NGFW-8786
If an external IGMP proxy is configured to use IGMP version 3 and an NGFW Engine IGMP proxy is configured to use IGMP version 2, multicast traffic might not be forwarded successfully.	FW	NGFW-8875

Description	Role	Issue number
If the Subject of a certificate request does not have a space after the comma, the NGFW Engine is not able to create the certificate request.	FW	NGFW-8935
If a policy that removes an interface or a VLAN interface is refreshed, the refresh might fail. The NGFW Engine might need to be restarted.	FW	NGFW-9014
When the NGFW Engine inspects certain types of traffic, memory consumption might increase substantially, inspected connections might experience high latency, or inspected connections might be dropped.	FW, IPS, L2FW	NGFW-9110
If a policy is installed or refreshed on an NGFW Engine that has a lot of static routes, all the static routes configured in the Management Client might not be present in the Quagga dynamic routing configuration.	FW	NGFW-9162
It might not be possible to delete a VPN SA in the VPN SA monitoring view in the Management Client. The following message is shown: "Failed to delete VPN SA. Failed to process delete requests".	FW	NGFW-9236
DHCP requests relayed by the NGFW Engine might not work correctly if the request packets are very large.	FW	NGFW-9275
When the traffic capture (tcpdump) feature is started or stopped on MOE10F4 (MOD-EM2-10G-SFP-4) or MO40F2 (MOD-40G-2) interface modules, there might be a short interruption in traffic.	FW, IPS, L2FW	NGFW-9434

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.

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.

CAUTION: If McAfee Endpoint Intelligence Agent (McAfee EIA) is configured on the NGFW Engine when you upgrade to version 6.3 or later, the NGFW Engine node is returned to the initial configuration state and stops processing traffic. You must remove the McAfee Endpoint Intelligence Agent (McAfee EIA) configuration and refresh the policy before you upgrade to version 6.3 or later. For more information, see Knowledge Base article 14093.

Note: Changes to category-based URL filtering in Forcepoint NGFW version 6.1 affect all existing users of category-based URL filtering. Legacy URL Situation elements can no longer be used in policies for Forcepoint NGFW version 6.1 or later. If rules in your policy contain legacy URL Situation elements, you must replace them with URL Category elements. See the *Forcepoint Next Generation Firewall Product Guide* for detailed instructions.

Note: Starting from Forcepoint NGFW version 6.2, the Anti-Spam feature is no longer supported. See Knowledge Base article 12394. If you require this feature, we recommend that you use the most recent Long-Term Support (LTS) version. See Knowledge Base article 10192. If you require a comprehensive Anti-Spam and Email Security solution, we recommend that you use Forcepoint Email Security Cloud.

- Upgrading to version 6.3 is only supported from version 5.10 or later. If you have an earlier version, first upgrade to version 5.10.
- Forcepoint NGFW version 6.3 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 6.3. See Knowledge Base article 10461.

Known issues

For a list of known issues in this product release, see Knowledge Base article 14124.

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.
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.

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*