FlexEdge Secure SD-WAN Engine

7.2.5

Release Notes

Revision A

Contents

About this release

This document contains important information about this release of Forcepoint FlexEdge Secure SD-WAN Engine. We strongly recommend that you read the entire document.

Product name change

Starting from Forcepoint FlexEdge Secure SD-WAN version 7.1 release the product name has changed from Forcepoint NGFW to Forcepoint FlexEdge Secure SD-WAN. The primary changes are listed below:

Component	Old name	New name
Solution	Forcepoint NGFW	Forcepoint FlexEdge Secure SD-WAN
Management	Security Management Center (SMC)	FlexEdge Secure SD-WAN Manager / SD-WAN Manager Console (SMC)
Engine	NGFW Engine	FlexEdge Secure SD-WAN Engine

Currently, product name change is visible in SMC and in the following documentations:

- *Forcepoint FlexEdge Secure SD-WAN Manager API User Guide*
- *Forcepoint FlexEdge Secure SD-WAN Installation Guide*
- *Forcepoint FlexEdge Secure SD-WAN Product Guide*
- *Forcepoint FlexEdge Secure SD-WAN online help*
- *Forcepoint FlexEdge Secure SD-WAN Quick Start Guide*

For more information on SMC UI terminology change, refer to the **About this Help** section in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

> **Note**
>
> 1) Some documentations, knowledge base articles, and other support information are still using the old product name.
>
> 2) There is no change in the Engine local user interface.
>
> 3) The IPS role has transitioned now from L2FW mode to L3FW mode.

Deprecated Features

Web Portal User Interface

Web Portal User Interface is deprecated and is not available by default. Web Portal Server is still available to host Web Access.

Monitoring third-party devices

Support for monitoring third-party devices in SMC is now discontinued.

Working with diagram elements

The diagram feature for generating a model of a network diagram in SMC UI is now discontinued.

VMware NSX Integration

Support for VMware NSX Integration in SMC is now discontinued.

Lifecycle model

This release of Secure SD-WAN Engine is a Feature Stream (FS) version.

Support for Feature Stream versions is discontinued when a new major version of Forcepoint NGFW is available.

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

For more information about the Secure SD-WAN Engine lifecycle policy, see https://support.forcepoint.com/ProductSupportLifeCycle.

System requirements

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

Secure SD-WAN Engine appliances

We strongly recommend using a pre-installed Secure SD-WAN Engine appliance for Secure SD-WAN installations.

Note

Some features are not available for all appliance models. See Knowledge Base article 9743 for appliance-specific software compatibility information.

The majority of the following supported appliances can be used in the Engine/VPN, or Engine with Layer 2 Interfaces.

- 60 Series (60, 60L, and 61)
- 120 Series (120, 120L, 120W, 120WL, and 125L)
- 330 Series (330, 331, and 335)
- 350 Series (352 and 355)
- 1100 Series (1101 and 1105)
- 1202
- 2100 Series (2101 and 2105)
- 2200 Series (2201, 2205, and 2210)
- 3300 Series (3301 and 3305)
- 3400 Series (3401, 3405, and 3410)
- 3500 Series (3510 and 3510)
- 6205

Note

To use the appliance as VPN Broker or with Forcepoint NGFW Manager, we recommend that you use a Secure SD-WAN Engine appliance that has at least 4GB of memory.

Basic hardware requirements

You can install Secure SD-WAN Engine on standard hardware with these basic requirements.

Component	Requirement
CPU	Intel® processors based on Westmere microarchitecture or newer.
Memory	Minimum 4 GB of RAM

Component	Requirement
Hard disk	Minimum 8 GB **Note** RAID controllers are not supported.
Peripherals	- DVD drive - VGA-compatible display - Keyboard
Interfaces	- One or more network interfaces for the Engine/VPN role - Two or more network interfaces for the IPS in IDS configuration - Three or more network interfaces for inline Engines with Layer 2 Interfaces For information about supported Ethernet interface types and adapters, see Knowledge Base article 9721.

Master Secure SD-WAN Engine requirements

Master Secure SD-WAN Engines have specific hardware requirements.

- Each Master Secure SD-WAN Engine must run on a separate physical device. For more details, see the *Forcepoint FlexEdge Secure SD-WAN Installation Guide*.
- All Virtual Secure SD-WAN Engines hosted by a Master Secure SD-WAN Engine or Master Secure SD-WAN Engine cluster must have the same role and the same Failure Mode (*fail-open* or *fail-close*).
- Master Secure SD-WAN Engines can allocate VLANs or interfaces to Virtual Secure SD-WAN Engines. If the Failure Mode of the Virtual IPS engines or Virtual Layer 2 Engines is *Normal* (fail-close) and you want to allocate VLANs to several Secure SD-WAN Engines, you must use the Master Secure SD-WAN Engine cluster in standby mode.
- Cabling requirements for Master Secure SD-WAN Engine clusters that host Virtual IPS engines or Layer 2 Engines:
  - Failure Mode *Bypass* (fail-open) requires IPS serial cluster cabling.
  - Failure Mode *Normal* (fail-close) requires Layer 2 Engine cluster cabling.

  For more information about cabling, see the *Forcepoint FlexEdge Secure SD-WAN Installation Guide*.

Virtual appliance node requirements

You can install Secure SD-WAN Engine on virtual appliances with these hardware requirements. Also be aware of some limitations.

Component	Requirement
CPU	Intel® processors based on Westmere microarchitecture or newer.
Memory	Minimum 4 GB of RAM
Virtual disk space	Minimum 8 GB

Component	Requirement
Hypervisor	One of the following: - VMware ESXi 6.5 or 7.0 - KVM with Red Hat Enterprise Linux 7.9 or 8.5 - (Engine/VPN role only) Microsoft Hyper-V on Windows Server 2016 with an Intel 64-bit processor
Interfaces	- At least one virtual network interface for the Engine/VPN role - Three virtual network interfaces for Engines with Layer 2 Interfaces The following network interface card drivers are recommended: - VMware ESXi platform — `vmxnet3`. - KVM platform — `virtio_net`.

When Secure SD-WAN Engine is run as a virtual appliance node in the Engine/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 Secure SD-WAN Engine is run as a virtual appliance node in the Engines with Layer 2 Interfaces, clustering is not supported.

Supported cloud environments

You can deploy Secure SD-WAN Engine in the Amazon Web Services (AWS) and Microsoft Azure cloud environments.

Google Cloud, IBM Cloud, and Oracle Cloud

Starting from Secure SD-WAN Engine version 6.11 public cloud platforms from Google, IBM, and Oracle are supported. For more details, see the Knowledge Base article 39116.

Amazon Web Services

Secure SD-WAN Engine instances can be launched from AWS using 1-Click Launch, and existing instances can be remotely upgraded to the latest Secure SD-WAN Engine version.

To see the currently available instance types, search for *Forcepoint Secure SD-WAN Engine* in the AWS Marketplace.

For more information about deploying in AWS, see the document *How to deploy FlexEdge Secure SD-WAN in the Amazon Web Services cloud* and Knowledge Base article 10156.

Microsoft Azure

Secure SD-WAN Engine instances can be launched from Azure using custom solution templates, and existing instances can be remotely upgraded to the latest Secure SD-WAN Engine version.

To see the currently available custom solution templates, search for *Forcepoint Secure SD-WAN Engine* in the Azure Marketplace.

For more information about deploying in Azure, see the document *How to deploy FlexEdge Secure SD-WAN in the Azure cloud* and Knowledge Base article 14485.

Build number and checksums

The build number for Secure SD-WAN Engine 7.2.5 is 30252.

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

- sg_engine_7.2.5.30252_x86-64-small.iso

  ```
  SHA256SUM:
  319bba020704b61a69a6503c92b2960d732f9d1030b148870c2986f266b7c575

  SHA512SUM:
  40b13a3955ebd86643220e78cb111263
  37d5706a9b5e5715d1a79c007a1beb3b
  c8ef1ac984141c4cb356ab0601f7c40e
  5b774ef7393ff181cdec1c1e799712ec
  ```

- sg_engine_7.2.5.30252_x86-64-small.zip

  ```
  SHA256SUM:
  502862fd152f778d7bf902ecf46e52e0d1205e7a4cffa6b200e51d6b126f1859

  SHA512SUM:
  9dba7e6ae98454fb599c59666cb38527
  2e394bc70e2d483ceb029598b009d674
  7685ab98c111ebffc0465dd09b0cffe5
  35e98b72b27ec21b1aeac9e64d8daa1b
  ```

- Forcepoint-NGFW-gencloud-7.2.5.30252.qcow2

  ```
  SHA256SUM
  8768ddbba554ee15bf9f9d75110fd4c850e093933acc67c3919b94d05d9150ad

  SHA512SUM
  9fb449cfda081733a4a55afc6c478243
  6620272143b0b5c0df5d4db8e321f28c
  9ea21d8c9790110a1bcd2f68d67b12cd
  fbde0fed9a3b608c16eabe448940af61
  ```

Compatibility

Secure SD-WAN Engine 7.2 is compatible with the following component versions.

- Forcepoint FlexEdge Secure SD-WAN Manager 7.2 or higher
- Dynamic Update 1814 or higher
- Forcepoint VPN Client 6.6.0 or higher for Windows

- Forcepoint VPN Client 2.0.0 or higher for Mac OS X
- Forcepoint VPN Client 2.0.0 or higher for Android
- Forcepoint VPN Client 2.5.0 or higher for Linux
- Server Pool Monitoring Agent 4.0.0 or higher
- Forcepoint Endpoint Context Agent (ECA) included in Forcepoint One Endpoint 19.05 or higher
- Forcepoint User ID Service 2.0.0 or higher

New features

This release of the product includes these new features. For more information and configuration instructions, see the *Forcepoint FlexEdge Secure SD-WAN Product Guide*, the *Forcepoint FlexEdge Secure SD-WAN Installation Guide*, and the *Forcepoint NGFW Manager and VPN Broker Product Guide*.

Starting from version 7.2.1, the following features are supported:

- **Adaptive Forward Erasure Correction (FEC) for SD-WAN tunnels**

  The FEC feature helps to control errors in data transmission over an unreliable or noisy communication channel.

  When FEC is enabled, the engine sends a combination of M data packets, N correction packets, and metadata information in a data set through a link to the destination. This allows recovering up to N missing data packets within one set of data and correction packets.

  For more information, see the *Adaptive Forward Erasure Correction (FEC) for SD-WAN tunnels* topic in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.
- **Backup unit support for single node engines**

  You can now configure hot standby backup unit for single node engines. This enables high availability configurations for scenarios that are only supported in single node engine, such as dynamic interfaces.

  For more information, see the *Configure a backup unit or a connection synchronization for external high availability* topic in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.
- **Connection Synchronization for External High Availability**

  You can now configure two separate single node engines to synchronize their connection tables. This enables building high availability (HA) setups where HA is controlled by an external entity, such as 3rd party load balancer.

  For more information, see the *Configure a backup unit or a connection synchronization for external high availability* topic in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Starting from version 7.2.0, the following feature is supported:

- **Multi-Link packet duplication**

By configuring the Multi-Link packet duplication feature you can enable duplication of traffic packets over multiple links that are sent to the same destination. This eliminates all packet loss due to link failure or delay in packet loss detection.

For more information, see the *Multi-Link packet duplication* topic in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Enhancements

This release of the product includes these enhancements.

Enhancements in Secure SD-WAN version 7.2.3

Enhancement	Description
New options to decrypt ESP and TLS traffic captures are added	New options are added to collect TLS keys and IPsec secrets with traffic capture to be able to decrypt captured traffic using Wireshark. These options can be utilized in troubleshooting. For more details: ■ On how to decrypt TLS traffic captures collected from the SD-WAN Engine, refer to the Knowledge Base article 11554. ■ On how to decrypt ESP packets captured from the Secure SD-WAN Engine, refer to the Knowledge Base article 11555.
Syslog forwarding can be added using the NGFW Manager	NGFW Manager configured Engine can be configured to forward syslog. Logs are sent over UDP in JSON format to a syslog server.
Explicit Proxy for HTTP and HTTPS connections	Users' web browser can be configured to use the SD-WAN Engine IP address as the HTTP(S) proxy server IP address. The feature supports proxy authentication. This feature is currently available for beta testing. For more information, see How to use the SD-WAN Engine Explicit HTTP Proxy.

Enhancements in Secure SD-WAN version 7.2.2

Enhancement	Description
Radius authentication for engine log in	It is now possible to configure engines so that local administrators are authenticated via RADIUS. Also, it is possible to control if the root admin can log in only from local console or via network using SSH. RADIUS authentications of engine supports access-challenge methods. **Note** This enhancement is only supported on engine versions 7.2.2 or later.
Support for inspection of Zstandard compressed traffic is added	Inspection process is able to decompress zstd encoded HTTP payload.

Enhancement	Description
Virtual Engine Binding Priority	The FlexEdge Secure SD-WAN engine is now enhanced so that Virtual Engine binding priority can be configured for Master Engines. The configuration can be done by using SMC. For more information, see the *How to Configure Virtual Engine Binding Priority in Master Engines* Knowledge Base Article.

Enhancements in Secure SD-WAN version 7.2.1

Enhancement	Description
Support for IPv6 address in the PPPoE interface is added	SMC managed single engine can now have both dynamic IPv4 and IPv6 addresses in its PPPoE interface. For more information, see the *Add point-to-point protocol clients to Single Engine interfaces* topic in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Enhancements in Secure SD-WAN version 7.2

Enhancement	Description
Legacy SNMP agent implementation removed	The legacy SNMP agent implementation has been removed on engine version 7.2 and later. Only the new enhanced version described in the *Enhanced SNMP Agent default in NGFW Engine version 7.0* Knowledge Base Article is available.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 42349 .

Security updates

For information about third-party packages and associated vulnerabilities included with the Engine in this product release, see Knowledge Base article 42351 .

Installation instructions

Use these high-level steps to install the SMC and the Secure SD-WAN Engines.

For detailed information, see the *Forcepoint FlexEdge Secure SD-WAN Installation Guide*. All guides are available for download at https://support.forcepoint.com/s/article/Documentation-Featured-Article.

Steps

1) Install the Management Server, the Log Servers.

2) Import the licenses for all components.

   You can generate licenses at https://stonesoftlicenses.forcepoint.com.

3) Configure the Engine elements in the Management Client from the **Configuration** view.

4) To generate initial configurations, right-click each Secure SD-WAN Engine, then select **Configuration** > **Save Initial Configuration**.

   Make a note of the one-time password.

5) Make the initial connection from the Secure SD-WAN Engines to the Management Server, then enter the one-time password.

6) Create and upload a policy on the Secure SD-WAN Engines in the Management Client.

Upgrade instructions

Take the following into consideration before upgrading licenses, Secure SD-WAN Engines, and clusters.

> **Note**
>
> Upgrading to version 7.2 is only supported from version 6.10 or higher. If you have a lower version, first upgrade to version 6.10.

- Secure SD-WAN version 7.2 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 Secure SD-WAN Engine, use the remote upgrade feature or reboot from the installation DVD and follow the instructions. For detailed instructions, see the *Forcepoint FlexEdge Secure SD-WAN Installation Guide*.

Find product documentation

In the Forcepoint Customer Hub, 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 in the Forcepoint Customer Hub at https://support.forcepoint.com. There, you can access product documentation, release notes, Knowledge Base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint Customer Hub. If you do not yet have credentials, create a customer account. To create a customer account, navigate to the Customer Hub Home page, and then click the **Create Account** link.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint FlexEdge Secure SD-WAN Product Guide*
- *Forcepoint FlexEdge Secure SD-WAN 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 FlexEdge Secure SD-WAN Installation Guide*

Other available documents include:

- *Forcepoint Hardware Guide* for your model
- *Forcepoint FlexEdge Secure SD-WAN Quick Start Guide*
- *Forcepoint FlexEdge Secure SD-WAN Manager API User Guide*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*
- *Forcepoint NGFW Manager and VPN Broker Product Guide*

Published 20 November 2025