Forcepoint

FlexEdge Secure SD-WAN Engine

7.1.14

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

This release changes the product name 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.

Lifecycle model

This release of Secure SD-WAN Engine 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 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.

Note

120W and 120WL appliances with hardware revision 2 or newer require Engine version 7.1.1 or newer. For more details about Appliance - Engine version compatibility please refer to https://support.forcepoint.com/s/article/Next-Generation-Firewall-appliance-software-support-table.

- 50 Series (51 and 51 LTE)
- 60 Series (60, 60L, and 61)
- 120 Series (120, 120L, 120W, 120WL, and 125L)
- 130 Series (130, 130W, and 130WL)
- 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)
- 2300 Series (2301, 2305, and 2310)
- 3300 Series (3301 and 3305)
- 3400 Series (3401, 3405, and 3410)
- 3500 Series (3505 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
Hard disk	Minimum 8 GB **Note** RAID controllers are not supported.
Peripherals	■ DVD drive ■ VGA-compatible display ■ Keyboard

Component	Requirement
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
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

Component	Requirement
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 7.1.14 is 29461.

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

- sg_engine_7.1.14.29461_x86-64-small.iso

```
SHA256SUM:
87f76ef9d536f3deadef964c8b6a45e00eef17d6ced5588fd9b891cb0fb98897

SHA512SUM:
350713414cbf45953bc0db85aadf7b56
0302b927471942da2e272f6319e17001
2daede7b0f1ef488265874f6f4734ddb
3b781b4d15264d711bee3c3d16781df3
```

- sg_engine_7.1.14.29461_x86-64-small.zip

```
SHA256SUM:
926e025b60e2dda4ad0caef300cacf7c884f7ab12d5a82cc507abb4072c8bdc3

SHA512SUM:
e3d8ff8772ed514fd8ddaf3a60468c15
47d706e156907b6f242bb1b38963d929
2a6d2eafc7c53f4add31c5e91de43177
6c9f59064a1b9a1cc3e79146ae70921c
```

- Forcepoint-NGFW-7.1.14.29461.qcow2

```
SHA256SUM:
540197da98a468f8fa26d682d029d82a54940605e4c7abb8be5a4d3c270b5a28

SHA512SUM:
9ee25b443a704c14d66b34a31831b089
f098b4bbd198503ede46b95d9f04906b
c4457f7a5c466064a37ed43d73e5f683
5c23bd0b1122cb976794506966260aae
```

Compatibility

Secure SD-WAN Engine 7.1 is compatible with the following component versions.

- Forcepoint FlexEdge Secure SD-WAN Manager 7.1 or higher
- Dynamic Update 1594 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*.

Forward traffic to specific tunnels or routers

By configuring the Forced Next Hop (FNH) option in the access rule you can now force forward traffic to a specific tunnel or router.

The advantage of using this option is that you can forward the matched traffic to a specific application that has the server behind a tunnel.

For more information, see *Configure Forced Next Hop routing* section in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

SMC contact via FQDN

You can now use FQDN as the contact address to enable the engine to contact the SMC management server or log server. This can be beneficial when you run the SMC management server or log server in a cloud environment where managing long term static public IP address is not feasible or is difficult.

For more information, see *Define Management Server or Log Server contact addresses*, and *Define contact address* sections in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

DNS Sinkholing

You can now configure DNS sinkholing for UDP and TCP service elements. One of the scenarios where this feature can be useful is, when there is an infected machine in the internal network. It can be identified by using the DNS sinkholing.

For more information, see *Create custom service elements* section in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Enhancements

This release of the product includes these enhancements.

Enhancements in Secure SD-WAN version 7.1.8

Enhancement	Description
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.

Enhancements in Secure SD-WAN version 7.1.7

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.

Enhancements in Secure SD-WAN version 7.1.4

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. **Note** This is only supported on SMC version 7.1.2 or later. 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*.
Support for inspection of Zstandard compressed traffic is added	Inspection process is able to decompress zstd encoded HTTP payload.

Enhancements in Secure SD-WAN version 7.1.3

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 SMC versions 7.1.4 or later, and 7.2.2 or later.
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 7.1.1

Enhancement	Description
Local Sandbox - Advanced Malware Detection & Protection option	You can now configure an Advanced Malware Detection & Protection local sandbox to detect advanced threats by analyzing the behavior of files in a restricted operating system environment. **Note** You need a local Advanced Malware Detection & Protection server to use this local sandbox service. For more information, see the *Connect Secure SD-WAN to a sandbox service* and the *Define Sandbox Service elements* sections in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Enhancements in Secure SD-WAN version 7.1

Enhancement	Description
BGP Monitoring Protocol (BMP) Configuration	You can now configure BMP options from the Dynamic Routing Editor. It is used to monitor BGP sessions and send the monitored data from BGP routers to the network management entities. Also, when configured the log events includes the information for the configured options, and which in turn helps to make correlation of BMP and engine logs easy for analytics. For more information, see *Create core elements for dynamic routing*, and *Enable BGP on the Engine, Engine Cluster, or Virtual Engine* sections in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.
Improved Application Health Monitoring	The Application Health Monitoring feature now comes with the following support: ■ Enhanced engine monitoring and better support for non-TCP traffic, that is there is now support for health monitoring of applications that use UDP for data transport. ■ Visibility into application health history and health status history of network applications. ■ Better ISP link status monitoring. ■ Application health status history. For more information, see *Application Health Monitoring Dashboard* section in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.
Improved SD-WAN algorithms and link selection logic	The following are tuned to provide better user experience: ■ Engine logic is updated to avoid too much packet loss before the traffic is sent to the better links. ■ The QoS link value selection feature was not working as intended. The QoS link value is tuned to make QoS link value selection feature to work as intended. Also, the **Default SD-WAN Link Balancing Preference** option is made available to allow you to set the preferences on how the traffic is balanced over the links for each engine. For more information, see *Create Link Usage Profile elements* section in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Enhancement	Description
Tunnel interface now supports multiple IP addresses	It is now possible to add multiple IP addresses (that can be of types IPv4 and IPv6) for tunnel interfaces.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 41767 .

Security updates

For information about third-party packages and associated vulnerabilities included with the Engine in this product release, see Knowledge Base article 41768 .

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 7.1 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 7.1 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 25 June 2026