

Course roadmap

This course contains the following modules:

1. Exploring the Engine
2. Reviewing the Secure SD-WAN Manager Console (SMC)
3. Getting Started with the Secure SD-WAN Manager Console (SMC)
4. Reviewing Policies and Templates
5. Configuring Access and NAT Rules
6. Introducing Traffic Inspection
7. Setting up Inspection Policies
8. Detecting Malware and Filtering Files
9. Configuring Alerts and Notifications
10. Managing Users and Authentication
11. Configuring the SSL VPN Portal
12. Configuring SD-WAN
13. Analyzing Logs
14. Utilizing Policy Tools
15. Monitoring Activity and Generating Reports
16. Introducing Troubleshooting Tools and Techniques
17. Installing a Single Engine
18. Exploring What's New in the Latest Product Release



Module 1

Exploring the Engine

- List the benefits and differentiators of Secure SD-WAN.
- Describe the Secure SD-WAN Engine and appliances.
- Differentiate between virtual engines and virtual appliances.
- Describe at least one of the installation methods.
- List the four common Secure SD-WAN deployments.

Module 2

Reviewing the Secure SD-WAN Manager

Console (SMC)

- Describe the Secure SD-WAN Manager console and its key features.
- Describe the Secure SD-WAN system architecture.
- Identify the ports used for communication between the SMC components.
- Explain the use of locations and contact addresses.
- Explain the use of SMC Domains.

Module 3

Getting Started with the Secure SD-WAN

Manager Console (SMC)

- Describe the management client and how it works.
- Create system backups.
- Describe the SMC high availability options.
- Configure the SMC Administrator Access.
- Apply configuration to Secure SD-WAN engines.
- Describe how logs work.

Module 4

Reviewing Policies and Templates

- Describe the types of Engine policies.
- Define Engine policy templates.
- Create an Engine policy hierarchy.
- Describe the benefits of aliases and continue rules.

Module 5

Configuring Access and NAT Rules

- Explain how traffic is matched in access rules.
- Explain the different types of access rules.
- Describe the actions for processing traffic in access rules.

- Explain the different types of NAT.
- Configure NAT rules.

Module 6

Introducing Traffic Inspection

- Explain the difference between a service, service with protocol, and proxy.
- Explain the enhanced access control methods.
- Explain different ways to control applications.
- List the detection methods used in the Engine Inspection.
- Describe advanced evasion techniques (AETs) and normalization.
- Describe TLS Inspection.
- Configure snort inspection on Engine.
- List the Forcepoint and third-party products that integrate with Forcepoint Engine.

Module 7

Setting up Inspection Policies

- Explain how to send traffic for deep packet inspection.
- Describe Forcepoint Engine situations and how to use them.
- Define the different type of rules in the inspection policy.
- Tune an inspection policy.

Module 8

Detecting Malware and Filtering Files

- List the different options for detecting malware.
- Explain how to send traffic for malware detection.
- Configure a file filtering policy.
- Integrate Forcepoint Engine with a Forcepoint Data Loss Prevention (DLP) system.

Module 9

Configuring Alerts and Notifications

- Explain the alert escalation process in Forcepoint Secure SD-WAN.
- Create an alert policy and alert chain to escalate an alert.

Module 10

Managing Users and Authentication

- Identify supported directory servers and authentication methods.
- Explain the browser-based user authentication mechanism.
- Configure user authentication.
- Differentiate between user authentication and user identification.

- Explain the difference between the Forcepoint UID and ECA.
- Configure user behavior monitoring.

Module 11

Configuring the SSL VPN Portal

- List Engine Mobile VPN Access options.
- Describe the SSL VPN Portal and the URL Rewrite translation method.
- Configure an SSL VPN Portal.

Module 12

Configuring SD-WAN

- Define the terms used by the Forcepoint SD-WAN feature.
- Explain how site-to-site SD-WANs work.
- Describe Full Mesh, Star, and Hub site-to-site SD-WAN topologies.
- List the SD-WAN features that Forcepoint Engine supports.
- Configure a policy-based SD-WAN.
- Describe how route-based SD-WANs work.

Module 13

Analyzing Logs

- Describe the log entry types available in Forcepoint Secure SD-WAN.
- Use the Management Client interface to interpret and analyze logs.
- Configure and manage logs.
- Create permanent filters.
- Analyze how pruning filters affect log data.
- Configure the log server to forward logs to third-party SIEM systems.
- Describe the methods available for managing the space consumed by log data.

Module 14

Utilizing Policy Tools

- Describe the benefits of Policy Snapshots.
- Search rules in a Secure SD-WAN policy.
- Analyze policy structure and apply tools to optimize access rules.

Module 15

Monitoring Activity and Generating Reports

- Monitor the system and engine activity.
- Describe the use of overviews in the SMC user interface.
- Configure and generate reports.
- Monitor Application Health.

Module 16

Introducing Troubleshooting Tools and Techniques

- Explain the troubleshooting process.
- Use the SMC for troubleshooting.
- Explain how to collect diagnostics for Technical Support.
- Resolve common SMC issues.
- Explain how engine packet processing works.

Module 17

Installing a Single Engine

- Describe engine deployment options.
- List features specific to single engines.
- Configure a single engine in the SMC.
- Configure an engine for initial contact with the SMC.
- Establish the trust between SMC and a newly installed engine.

Module 18

Exploring What's New in the Latest Product Release