Forcepoint Web Security System Engineer Instructor-Led

Datasheet

August 2020

Forcepoint

forcepoint.com

Forcepoint Web Security System Engineer Instructor-Led Training

WBIMP

During this five-day classroom-based instructor-led course, you will gain an understanding of the core competencies and skills needed to practice as a system engineer handling Forcepoint Web Security.
The core competencies are design and deployment, component implementation, troubleshooting, and debugging.
This course prepares engineers or other professionals who are about to manage or lead system engineering development of Forcepoint Web Security from concept creation to production.

Audience

- Channel Partners: Sales Engineers, Implementation Specialists, Deployment Specialists, Network Architects, Technical Support
- Customers: Deployment Specialists, Implementation Specialists, System Engineers
- Forcepoint: Sales Engineers, Professional Services, Technical Support

Format:

Classroom Instructor-Led Training

Duration:

40 hours, typically delivered in 5 sessions/8 hours per session

Course Price:

$3,500 USD non-discountable

Exam Price:

One attempt is included

Course objectives

- Analyze key deployment considerations
- Calculate sizing and performance tuning
- Classify different deployment types
- Install and configure Web Security with appliances
- Assess how Web Security integrates with supported third-party solutions
- Configure tweaks to tune and balance settings to respond to daily needs
- Perform troubleshooting and debugging

Prerequisites for attendance

- Completion of the Forcepoint Web Administrator Course and certification
- Intermediate knowledge of networking and computer security concepts
- A computer that meets the requirements noted at the end of this document

Certification exams

This course prepares you to take and pass the Certified Forcepoint Web Security System Engineer exam. The exam is included in the price of the course. The Web Security System Engineer exam is a two-part exam:
Theoretical (multiple choice) and Practical (hands-on). Both exams will be administered on Session 5 of the course.
A minimum score of 80% on the multiple-choice online exam and a 70% of the Hands-on exam is required to obtain the System Engineer certification.

Course Outline

Module 1: Deployment

- Identify which services and components to install.
- Follow best practices to review installation prerequisites.
- Describe the Forcepoint appliance architecture.
- Complete a Web Security installation on a Windows host.
- Find relevant logs if deployment issues arise.
- Apply guidelines related to component placement, limits, ratios, and supported configurations.
- Complete an initial appliance setup.
- Identify features of Forcepoint appliances.
- Define methods of traffic redirection using Content Gateway.
- Identify explicit and transparent proxies.
- Describe methods of configuring the proxy for high availability.
- Explain various deployment workflow for simple, medium, and advanced network deployments.
- Utilize the recommended sizing guidelines and list deployment recommendations for small, medium, and large networks.
- Identify supported Forcepoint solutions and third-party products for integration.
- Explain policy migration from Web Security on-premises to Web Security Cloud.
- List considerations and required components needed for disaster recovery.
- Follow applicable disaster recovery guidelines.

Module 2: Configuration

- Identify Web Security components and their interconnectivity.
- Specify the components that support bare minimum deployments.
- Explain key services and settings that support Web Security components.
- Install and use Forcepoint Security Appliance Manager.
- Identify and analyze filtering and policy enforcement components.
- Articulate essential features and functions about the Content Gateway architecture.
- Design and implement proxy authentication based on a customer’s network size and Directory Service options.
- Implement user identification components in single and multi-domain environments.
- Describe User Service.
- Explain SIEM integration.

Module 3: Troubleshooting and Debugging

- Identify Web Security configuration files, diagnostic tools, tuning parameters, and verbose logging.
- List general recommendations when troubleshooting issues and formulating workarounds.
- Locate specific Web Security logs.
- Follow steps to use Visual Diagnostic Tool.
- Describe available options and tools when gathering diagnostic data for Web Security components.
- Interpret debug.txt results.
- Demonstrate appliance CLI commands and operations.

Terms and Conditions

- This course is limited to the topics described in this datasheet and may not address all of your unique requirements.
- Forcepoint trainings are standard and non-negotiable.
- Forcepoint provides the training “AS IS” and makes no warranties of any kind, express or implied.
- System Engineer courses must be completed within six months from purchase or the course may be forfeited.
- The training services in this course are provided pursuant to the Subscription Agreement.
- Assent to the Subscription Agreement constitutes acceptance of the above terms and conditions.

For more information about this course or other Forcepoint training offerings, please visit https://www.forcepoint.com/services/training-and-technical-certification or contact Forcepoint Technical Learning Services at learn@forcepoint.com.

Forcepoint