FORCEPOINT
POWERED BY Raytheon

FORCEPOINT WEB SECURITY

System Engineer Course Data Sheet

FORCEPOINT WEB SECURITY

SYSTEM ENGINEER COURSE

Intended audience

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

Format

- Instructor-Led Training (classroom training)

Duration

- 5 days, 8 hours per day

Pre-requisites

- Completion of the Forcepoint Web Security Administrator Course

Certification requirements

- Completion of all course sessions
- Configured lab exercises
- Certification exam (multiple choice and hands-on)

Overview

- During the five days, students will gain an understanding of the key core competencies and skills needed to practice as a System Engineer handling Forcepoint Web Security. The core competencies are sizing, deployment, product tuning, and troubleshooting.
  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.

Course objectives

- Understand key deployment considerations
- Learn about sizing and performance tuning
- Understand different deployment types
- Understand how Web Security integrates with supported third-party solutions
- Configure tweaks to tune and balance settings to respond to daily needs
- Learn about troubleshooting and debugging

Day 1 – Deployment

1) **Key Considerations**
   a) Minimum and Recommended Hardware and Software Requirements
   b) Placement
   c) Components Deployment
   d) External Services Integration
2) **Deployment Methodologies**
   a) Simple Network Deployments
   b) Intermediate Network Deployments

Day 2 – Deployment (Cont.) and TRITON Infrastructure

1) **Deployment Methodologies**
   a) Advanced Network Deployments
2) **Sizing**
3) **Installation Flow**
   a) Installation Verification
   b) Installation Footprint

Day 3 – Components Implementation

1) **TRITON Infrastructure**
2) **Components**
   a) Filtering and Policy
   b) User Identification
   c) Logging and Reporting
3) **Content Gateway**
   a) Proxy Modules
4) **Implementing Proxy Authentication**
5) **Managing Encrypted Traffic**

Day 4 –Troubleshooting and Debugging

1) **Troubleshooting**
   a) TRITON Manager
   b) Filtering and Policy Components
   c) User Service
   d) Log Server
   e) Content Gateway

Day 5 –Troubleshooting (Cont.) and Debugging

1) **Disaster Recovery**
   a) Key Considerations
   b) Best Practices
2) **Troubleshooting Methodologies**
   a) Investigating Symptoms
   b) Identifying Affected Areas/Components
   c) Determining what has changed
   d) Selecting the Most Probable Cause
   e) Implementing a Solution
   f) Recognizing Potential Effects of the Solution
   g) Testing the Solution
   h) Document the Solution

For more information about other Forcepoint training offerings, please visit our Customer or Partner training page.

Questions about Forcepoint training? Contact Forcepoint Technical Readiness and Training at salestraining@forcepoint.com