Forcepoint Web Security Administrator

Length 3 Days

Description

During the three days, students will learn the features, components, and key integrations that enable the Forcepoint Web Security functionalities. The course covers policy creation, incident management, and health assessment of the Forcepoint Web Security system. Students will develop skills in web policy creation, incident management, reporting, system architecture, and maintenance.

Certification requirements
- Completion of all course sessions
- Configured lab exercises
- Certification exam (multiple choice)

Participants

End-User/Customers: System administrators, network security administrators, IT staff,
Channel Partners: Sales Engineers, consultants, implementation specialists

Objectives

Understand the Forcepoint Web Security Components & Architecture
- Understand common deployment topologies
- Configure TRITON Manager
- Learn to update and upgrade Forcepoint Web Security
- Understand delegated administration
- Understand policy and filter basics
- Perform policy planning tasks
- Create effective web policies
- Understand exception management
- Understand different user management methods
- Configure user identification and policy enforcement
- Create notifications and alerts
- Understand report types and utilization
- Create various reports
- Understand system health alerts and usage monitor
- Understand system disaster recovery procedures
- Learn how to respond to incidents

Programme

Topic 1
1) Introductions
a) Participant Introductions
b) Logistics
c) Course Objectives

2) Forcepoint Web Security Overview
a) Forcepoint Solution Overview
b) What's New

3) Forcepoint Web Security Components and Architecture
a) Web Filter and Security
b) Management
c) Logging/Reporting
d) Integration
e) Appliance Overview

4) Sample Deployments and Best Practices
a) Deployment Types and Comparison
b) Sample Deployments

Topic 2
1) TRITON Manager
a) TRITON Manager Basics
b) Delegated Administration

2) Licensing
a) Subscription Keys

3) Updates / Upgrades
a) Server Component and Appliance Upgrade
b) Upgrade Resources
c) Best Practices

4) Policy Management
a) Policy and Filter Basics
b) Policy Planning and Creation
c) Exception Management
d) Best Practices

Topic 3
1) User Management
a) User Accounts Overview
b) Off-site User Management
c) User Identification and Policy Enforcement
d) Best Practices

2) Notifications
a) Alerting Basics
b) Best Practices

3) Reports
a) Report Basics
b) Report Interpretation
c) Best Practices

Topic 4
1) System Health and Logs
a) Health Alerts and Usage Monitor
b) Best Practices

2) Disaster Recovery
a) Backup and Restore
b) Best Practices

3) Incident Response
a) Issues and Best Responses

Options

Certification requirements
- Completion of all course sessions
- Configured lab exercises
- Certification exam (multiple choice)