optima
PROFESSIONAL SERVICES

Forcepoint Web Security Administrator Course (VILT) Outline

Forcepoint Web Security

Administrator Course

Intended audience:

• End-User/Customers: System administrators, network security administrators, IT staff

• Channel Partners: Sales Engineers, consultants, implementation specialists

Format	Duration	Prerequisites	Certification Requirements
Instructor Led-Training (Virtual)	4 Days	• General understanding of system administration and Internet services • Basic knowledge of networking and computer security concepts • A computer that meets the requirements noted at the end of this document	• Completion of all course sessions • Configured lab exercises and homework assignments • Certification exam (multiple choice)

Overview:

During the four 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.

Course objectives:

- Identify and retell the Forcepoint Web Security components and architecture
- Diagram common deployment topologies
- Access and use Security Manager, including other available user interfaces

- Execute updates and upgrades on Forcepoint Web Security
- Understand delegated administration
- Create effective web policies
- Understand exception management
- Differentiate various user management methods
- Configure user identification and policy enforcement
- Create notifications and alerts
- Generate various report
- Create various reports
- Define system health alerts and usage monitoring
- Understand system disaster recovery procedures
- Create incident response plans

Course Outline:

Module 1: Understanding and Getting Started with Web Security ▸ Web Security Overview ▸ Components and Architecture ▸ Appliance Overview	**Module 2: Policy Enforcement and Filtering** ▸ Policy Management ▸ Advanced Analysis ▸ Policy Enforcement
Module 3:Monitoring Web Security Activities ▸ Notifications and Alerts ▸ Reports	**Module 4: Disaster Response and Recovery** ▸ Incident Response ▸ System Health and Logs ▸ Updates and Upgrades ▸ Disaster Recovery

optima
PROFESSIONAL SERVICES

Module 1: Understanding and Getting Started with Web Security

- Articulate the key features and functions of Web Security
- Describe features, components, and key integrations that enable Web Security functionalities
- Compare the advantages and disadvantages of various deployment methodologies
- Articulate the licensing structure and how and when to enter the key within the Content Gateway
- Distinguish the key settings in Security Manager, Content Gateway Manager, Forcepoint Security Appliance Manager, and other available user interfaces
- Describe the differences between Super Administrators and delegated administrators

Module 2: Policy Enforcement and Filtering

- Describe the full scope and workflow of policy planning
- Identify standard and custom policies (and related filters) based on your organizations needs
- Distinguish the key settings in Security Manager
- Compare user identification and proxy authentication
- Explain how Web Security analyses user requests and enforces policies

Module 3: Monitoring Web Security Activities

- Itemize the available notifications and alerts
- Explain the reporting flow
- Describe the various reporting options to gain important insights about your environment
- Identify suspicious network activity using threats dashboard
- Compare the available reporting tools, including legacy and Report Center features

Module 4: Disaster Response and Recovery

- Explain how Web Security responds to incidents
- Compare and contrast the available update options
- Distinguish the guidelines related to incident management and disaster recovery
- Identify system health monitoring capabilities
- Complete various tasks that will help maintain a healthy Web Security environment
- Define the best practice procedures for disaster recovery