Forcepoint Web Security Administrator e-Learning

This eLearning course provides in-depth instruction where 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.

**Audience**

- Consultants, system architects, integrators and planners who help customers with Forcepoint Insider Threat implementations
- System administrators, network security administrators, IT staff and Forcepoint Web Security Operators

**Course objectives**

- Understand the Forcepoint Web Security Components & Architecture
- Articulate common deployment topologies
- Access and use Security Manager, including other available user interfaces
- Execute updates and upgrades on Forcepoint Web Security
- Understand delegated administration
- Comprehend and perform policy and filter basics
- Create effective web policies
- Understand exception management
- Configure user identification and policy enforcement
- Create notifications and alerts
- Understand report types and utilization to be able to respond to incidents
- Create various reports
- Understand system health alerts and usage monitoring
- Understand system disaster recovery procedures

**Prerequisites for attendance**

- 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.

**Certification exams**

This course prepares you to take and pass the Certified Forcepoint Web Administrator Exam. The exam can be purchased separately at a rate of $100. If you would like to take the certification exam following completion of the eLearning course, please contact learn@forcepoint.com for purchase details.

“I have been using Forcepoint products for 2 years, this course really filled in the gaps.”
Course Outline

MODULE 1: INTRODUCTION
- Overview of what will be covered in this course and the objectives
- Review lab environment and the commonly used interfaces
- How to use the student guide

MODULE 2: OVERVIEW ARCHITECTURE & DEPLOYMENT
- Articulate the key features and functions of Forcepoint 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
- Understand the difference and access rights for Super Administrators vs/ Delegated Administrators

MODULE 3: GLOBAL ADMINISTRATION AND POLICY CONFIGURATIONS
- Utilize the Master Database to select standard filters and create custom filters
- Understand the full scope and workflow of policy planning
- Define custom and standard policies based on your organizations needs
- Distinguish the key settings in the Security Manager
- Describe the infrastructure of SSL (Secure Sockets Layer) and TLS (Transport Layer Security)
- Perform URL filtering and analysis
- Understand User Identification & Forcepoint Content Gateway Authentication
- Understand how Web Security manages user requests and enforces policies

MODULE 4: POLICY ENFORCEMENT, NOTIFICATIONS AND REPORTS
- Set up notifications and alerts in order to be informed about various incidents and activities
- Understand the Reporting Flow
- Utilize the various reporting options to gain important insights about your environment
- Obtain exposure on Content Gateway scanning and various Web Security reporting tools
- Investigate suspicious network activity using threats dashboard

MODULE 5: SYSTEM HEALTH AND DISASTER RECOVERY
- Understanding incidents and leveraging Web Security to respond to incidents such as minor disasters
- Perform Web Security upgrades and hotfixes
- Compare and contrast Web Security update options
- Appropriately utilize the guidelines related to incident management and disaster recovery
- Identify system health monitoring capabilities
- Perform various tasks that will help maintain a healthy Web Security environment
- Utilize best practices procedures for disaster recovery
MODULE 6: WHAT'S NEW IN V8.5
- Identify the new features, enhancements, and other changes available in Web Security version 8.5
- Describe the benefits of the new features

MODULE 7: WHAT'S NEW IN V8.5.3
- Identify the new features, enhancements, and other changes available in Web Security version 8.5.3
- Describe the benefits of the new features

*To attend this e-Learning course, you must have a computer with:
- A high-speed internet connection (minimum of 1MB connection required)
- An up to date web browser (Google Chrome recommended)
- Adobe Flash web browser plug in (v13 or higher)
- PDF Viewer
- Speakers and microphone or headset (headset recommended)

Terms and conditions
Forcepoint products may be used to address customer concerns regarding content that could be considered objectionable or offensive. As a result, portions of Forcepoint course materials and lab exercises that train on these products may use examples of such content to teach appropriate protection mechanisms. Enrollees should be aware of this possibility, and if they are concerned should not enroll in this course or should consider purchasing a custom course that could be created to utilize other examples.

Additional terms and conditions found here: https://www.forcepoint.com/resources/training/forcepoint-training-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