Securing the Web with Cisco Web Security Appliance v3.1

The **Securing the Web with Cisco Web Security Appliance (SWSA)** course shows you how to implement, use, and maintain Cisco® Web Security Appliance (WSA), powered by Cisco Talos, to provide advanced protection for business email and control against web security threats. Through a combination of expert instruction and hands-on practice, you'll learn how to deploy proxy services, use authentication, implement policies to control HTTPS traffic and access, implement use control settings and policies, use the solution's anti-malware features, implement data security and data loss prevention, perform administration of Cisco WSA solution, and more.

This course helps you prepare to take the exam, Securing the Web with Cisco Web Security Appliance (300-725 SWSA), which leads to CCNP® Security and the Cisco Certified Specialist - Web Content Security. This course also earns you 16 Continuing Education (CE) credits towards recertification.

Training recipients

The training is aimed at:
- Security architects
- System designers
- Network administrators
- Operations engineers
- Network managers, network or security technicians, and security engineers and managers responsible for web security
- Cisco integrators and partners

Benefits

This class will help you:

- Implement Cisco WSA to secure web gateways, provide malware protection, and use policy controls to address the challenges of securing and controlling web traffic
- Gain valuable hands-on skills focused on web security
- Earn 16 CE credits toward recertification

Training program

Course Outline

- Describing Cisco WSA
- Deploying Proxy Services
- Utilizing Authentication
- Creating Decryption Policies to Control HTTPS Traffic
- Understanding Differentiated Traffic Access Policies and Identification Profiles
- Defending Against Malware
- Enforcing Acceptable Use Control Settings
- Data Security and Data Loss Prevention
- Performing Administration and Troubleshooting
- References

Lab Outline

- Configure the Cisco Web Security Appliance
- Deploy Proxy Services
- Configure Proxy Authentication
- Configure HTTPS Inspection
- Create and Enforce a Time/Date-Based Acceptable Use Policy
- Configure Advanced Malware Protection
- Configure Referrer Header Exceptions
- Utilize Third-Party Security Feeds and MS Office 365 External Feed
- Validate an Intermediate Certificate
- View Reporting Services and Web Tracking
- Perform Centralized Cisco AsyncOS Software Upgrade Using Cisco SMA

Expected preparation of the participant

To fully benefit from this course, you should have knowledge of these topics:
- TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
- IP routing

You are expected to have one or more of the following basic technical competencies or equivalent knowledge:
- Cisco certification (CCENT certification or higher)
- Relevant industry certification [International Information System Security Certification Consortium ((ISC)2), Computing Technology Industry Association (CompTIA) Security+, International Council of Electronic Commerce Consultants (EC-Council), Global Information Assurance Certification (GIAC), ISACA]
- Cisco Networking Academy letter of completion (CCNA® 1 and CCNA 2)
- Windows expertise: Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE)], CompTIA (A+, Network+, Server+)

Training Includes

2 days of web-based classes with hands-on lab practice

Language

- Training: English
- Materials: English

Czas trwania

2 dni / 14 godzin

Examination description

The training prepares you for the 300-725 SWSA exam, which can be taken for an additional fee at the PearsonVUE center. You can also take the exam on-line.

Details are available at: https://home.pearsonvue.com/cisco/onvue