Securing the Web with Cisco Web Security Appliance (SWSA)

Duration: 2 days

Who should attend?

1. Security architects
2. System designers
3. Network administrators
4. Operations engineers
5. Network managers, network or security technicians, and security engineers and managers responsible for web security
6. Cisco integrators and partners

Certifications

This course is part of the following Certifications:

1. Cisco Certified Network Professional Security (CCNP)

Prerequisites

To fully benefit from this course, you should have knowledge of these topics:

1. TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
2. IP routing

You are expected to have one or more of the following basic technical competencies or equivalent knowledge:

1. Cisco certification (CCENT certification or higher)
2. 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]
3. Cisco Networking Academy letter of completion (CCNA 1 and CCNA 2)
4. Windows expertise: Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE)], CompTIA (A+, Network+, Server+)

Certification: (300-725 SWSA), which leads to CCNP® Security and the Cisco Certified Specialist - Web Content Security certifications.

Course Objectives

The Securing the Web with Cisco Web Security Appliance (SWSA) v3.0 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 class will help you:

1. **Implement Cisco WSA to secure web gateways, provide malware protection, and use policy controls to address the challenges of securing and controlling web traffic**
2. **Gain valuable hands-on skills for high-demand responsibilities focused on web security**

After taking this course, you should be able to:

1. **Describe Cisco WSA**
2. **Deploy proxy services**
3. **Utilize authentication**
4. **Describe decryption policies to control HTTPS traffic**
5. **Understand differentiated traffic access policies and identification profiles**
6. **Enforce acceptable use control settings**
7. **Defend against malware**
8. **Describe data security and data loss prevention**
9. **Perform administration and troubleshooting**

Course Content

1. **Describing Cisco WSA**
2. **Deploying Proxy Services**
3. **Utilizing Authentication**
4. **Creating Decryption Policies to Control HTTPS Traffic**
5. **Understanding Differentiated Traffic Access Policies and Identification Profiles**
6. **Defending Against Malware**
7. **Enforcing Acceptable Use Control Settings**
8. **Data Security and Data Loss Prevention**
9. **Performing Administration and Troubleshooting**
10. **References**