IT-SWSA - Securing the Web with Cisco Web Security Appliance

Cisco - CCNP Security - Networking

Durata:	Lingue:	Certificazione:
2 Giorni	**Italiano**	**Cisco Certified Network Professional Security**

Descrizione del corso

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 course helps you prepare to take the 300-725 SWSA exam, one of the six concentration exams that you can choose after 350-701 SCOR exam to achieve the CCNP Security certification. The 300-725 SWSA exam will be available on February 24, 2020.

Programma

Describing Cisco WSA
o Technology Use Case
o Cisco WSA Solution
o Cisco WSA Features
o Cisco WSA Architecture
o Proxy Service
o Integrated Layer 4 Traffic Monitor
o Data Loss Prevention
o Cisco Cognitive Intelligence
o Management Tools

ITCore Group

Via Balestra, 12
6900 Lugano (CH)
+41.091.9760019
www.itcoregroup.com

Via Lanino, 36
21047 Saronno (VA)
+39.02.84108669
www.itcoregroup.com

o Cisco Advanced Web Security Reporting (AWSR) and Third-Party Integration
o Cisco Content Security Management Appliance (SMA)
Deploying Proxy Services
o Explicit Forward Mode vs. Transparent Mode
o Transparent Mode Traffic Redirection
o Web Cache Control Protocol
o Web Cache Communication Protocol (WCCP) Upstream and Downstream Flow
o Proxy Bypass
o Proxy Caching
o Proxy Auto-Config (PAC) Files
o FTP Proxy
o Socket Secure (SOCKS) Proxy
o Proxy Access Log and HTTP Headers
o Customizing Error Notifications with End User Notification (EUN) Pages
Utilizing Authentication
o Authentication Protocols
o Authentication Realms
o Tracking User Credentials
o Explicit (Forward) and Transparent Proxy Mode
o Bypassing Authentication with Problematic Agents
o Reporting and Authentication
o Re-Authentication
o FTP Proxy Authentication
o Troubleshooting Joining Domains and Test Authentication
o Integration with Cisco Identity Services Engine (ISE)
Creating Decryption Policies to Control HTTPS Traffic
o Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Inspection Overview
o Certificate Overview
o Overview of HTTPS Decryption Policies
o Activating HTTPS Proxy Function
o Access Control List (ACL) Tags for HTTPS Inspection
o Access Log Examples
Understanding Differentiated Traffic Access Policies and Identification Profiles

o Overview of Access Policies
o Access Policy Groups
o Overview of Identification Profiles
o Identification Profiles and Authentication
o Access Policy and Identification Profiles Processing Order
o Other Policy Types
o Access Log Examples
o ACL Decision Tags and Policy Groups
o Enforcing Time-Based and Traffic Volume Acceptable Use Policies, and End User Notifications

Defending Against Malware
o Web Reputation Filters
o Anti-Malware Scanning
o Scanning Outbound Traffic
o Anti-Malware and Reputation in Policies
o File Reputation Filtering and File Analysis
o Cisco Advanced Malware Protection
o File Reputation and Analysis Features
o Integration with Cisco Cognitive Intelligence

Enforcing Acceptable Use Control Settings
o Controlling Web Usage
o URL Filtering
o URL Category Solutions
o Dynamic Content Analysis Engine
o Web Application Visibility and Control
o Enforcing Media Bandwidth Limits
o Software as a Service (SaaS) Access Control
o Filtering Adult Content

Data Security and Data Loss Prevention
o Data Security
o Cisco Data Security Solution
o Data Security Policy Definitions
o Data Security Logs

Performing Administration and Troubleshooting
o Monitor the Cisco Web Security Appliance
o Cisco WSA Reports
o Monitoring System Activity Through Logs

o System Administration Tasks
o Troubleshooting
o Command Line Interface
References
o Comparing Cisco WSA Models
o Comparing Cisco SMA Models
o Overview of Connect, Install, and Configure
o Deploying the Cisco Web Security Appliance Open Virtualization Format (OVF) Template
o Mapping Cisco Web Security Appliance Virtual Machine (VM) Ports to Correct Networks
o Connecting to the Cisco Web Security Virtual Appliance
o Enabling Layer 4 Traffic Monitor (L4TM)
o Accessing and Running the System Setup Wizard
o Reconnecting to the Cisco Web Security Appliance
o High Availability Overview
o Hardware Redundancy
o Introducing Common Address Redundancy Protocol (CARP)
o Configuring Failover Groups for High Availability
o Feature Comparison Across Traffic Redirection Options
o Architecture Scenarios When Deploying Cisco AnyConnect® Secure Mobility
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