

Das Training zeigt Ihnen, wie Sie die Cisco® Web Security Appliance (WSA), powered by Cisco Talos, implementieren, verwenden und warten, um einen erweiterten Schutz für Geschäfts-E-Mails und die Kontrolle gegen Web-Sicherheitsbedrohungen zu bieten. Durch eine Kombination aus fachkundiger Anleitung und praktischer Übung lernen Sie, wie Sie Proxy-Dienste bereitstellen, Authentifizierung verwenden, Richtlinien zur Kontrolle des HTTPS-Verkehrs und - Zugriffs implementieren, Einstellungen und Richtlinien zur Nutzungskontrolle implementieren, die Anti-Malware-Funktionen der Lösung nutzen, Datensicherheit und Datenverlustvermeidung implementieren, die Verwaltung der Cisco WSA-Lösung durchführen und vieles mehr.

Kursinhalt

- 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

E-Book Sie erhalten die englischen Original-Unterlagen als Cisco E-Book. Bei der Cisco Digital Learning Version sind die Inhalte der Kursunterlage stattdessen in die Lernerfläche integriert.

Zielgruppe

- Security Architekten
- System Designer
- Netzwerk Administratoren
- Operation Engineers
- Netzwerk-Manager
- Netzwerk oder Security Techniker und Security Engineers und Manager
- Cisco-Integratoren und -Partner

Voraussetzungen

Sie sollten über Kenntnisse in diesen Bereichen verfügen:

- TCP/IP-Dienste, einschließlich Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP und HTTPS.
- IP-Routing

Eine oder mehrere der folgenden technischen Grundkompetenzen oder gleichwertige Kompetenzen sollten vorhanden sein:

- Cisco-Zertifizierung (CCENT-Zertifizierung oder höher)
- Relevante Branchenzertifizierung (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).
- Abschluss der Cisco Networking Academy (CCNA® 1 und CCNA 2)
- Windows-Know-how: Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE)], CompTIA (A+, Network+, Server+)

Kursziel

Dieser Kurs hilft Ihnen bei der Vorbereitung auf die Prüfung Securing the Web with Cisco Web Security Appliance, die Bestandteil des CCNP® Security ist und zudem zum Cisco Certified Specialist - Web Content Security führt.

Bearbeitungszeit

ca. 12 Stunden

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/SWSA

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Cisco Digital Learning & Cisco U.

Die multimodalen Schulungen der Cisco Digital Learning Library beinhalten referenzgeführte HD-Videos mit hinterlegtem durchsuchbarem Text und Untertiteln, Übungen, Labs und erklärenden Text sowie Grafiken. Das Angebot stellen wir Ihnen über unser Lernportal myExperTeach zur Verfügung. Der Zugriff auf die Kurse steht ab der Freischaltung für einen Zeitraum von sechs Monaten zur Verfügung. Bei Paketen (Cisco U.) beträgt dieser Zeitraum zwölf Monate.

Cisco Digital Learning & Cisco U. Preise zzgl. MwSt.

6 Monate Freischaltung **CHF 550,-**

Training Preise zzgl. MwSt.

Termine in Deutschland 2 Tage CHF 2.195,-

Online Training 2 Tage CHF 2.195,-

Termin/Kursort Kurssprache Deutsch

31.03.-01.04.25 Frankfurt 18.08.-19.08.25 Online

31.03.-01.04.25 Online 15.12.-16.12.25 Frankfurt

18.08.-19.08.25 Frankfurt 15.12.-16.12.25 Online



Inhaltsverzeichnis

SWSA – Securing the Web with Cisco Web Security Appliance

Describing Cisco WSA

- Technology Use Case
- Cisco WSA Solution
- Cisco WSA Features
- Cisco WSA Architecture
- Proxy Service
- Integrated Layer 4 Traffic Monitor
- Data Loss Prevention
- Cisco Cognitive Intelligence
- Management Tools
- Cisco Advanced Web Security Reporting (AWSR) and Third-Party Integration
- Cisco Content Security Management Appliance (SMA)

Deploying Proxy Services

- Explicit Forward Mode vs. Transparent Mode
- Transparent Mode Traffic Redirection
- Web Cache Control Protocol
- Web Cache Communication Protocol (WCCP) Upstream and Downstream Flow
- Proxy Bypass
- Proxy Caching
- Proxy Auto-Config (PAC) Files
- FTP Proxy
- Socket Secure (SOCKS) Proxy
- Proxy Access Log and HTTP Headers
- Customizing Error Notifications with End User Notification (EUN) Pages

Utilizing Authentication

- Authentication Protocols
- Authentication Realms
- Tracking User Credentials
- Explicit (Forward) and Transparent Proxy Mode
- Bypassing Authentication with Problematic Agents
- Reporting and Authentication
- Re-Authentication
- FTP Proxy Authentication
- Troubleshooting Joining Domains and Test Authentication
- Integration with Cisco Identity Services Engine (ISE)

Creating Decryption Policies to Control HTTPS Traffic

- Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Inspection Overview
- Certificate Overview
- Overview of HTTPS Decryption Policies

- Activating HTTPS Proxy Function
- Access Control List (ACL) Tags for HTTPS Inspection
- Access Log Examples

Understanding Differentiated Traffic Access Policies and Identification Profiles

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

Defending Against Malware

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

Enforcing Acceptable Use Control Settings

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

Data Security and Data Loss Prevention

- Data Security
- Cisco Data Security Solution
- Data Security Policy Definitions
- Data Security Logs

Performing Administration and Troubleshooting

- Monitor the Cisco Web Security Appliance
- Cisco WSA Reports

- Monitoring System Activity Through Logs
- System Administration Tasks
- Troubleshooting
- Command Line Interface

References

- Comparing Cisco WSA Models
- Comparing Cisco SMA Models
- Overview of Connect, Install, and Configure
- Deploying the Cisco Web Security Appliance Open Virtualization Format (OVF) Template
- Mapping Cisco Web Security Appliance Virtual Machine (VM) Ports to Correct Networks
- Connecting to the Cisco Web Security Virtual Appliance
- Enabling Layer 4 Traffic Monitor (L4TM)
- Accessing and Running the System Setup Wizard
- Reconnecting to the Cisco Web Security Appliance
- High Availability Overview
- Hardware Redundancy
- Introducing Common Address Redundancy Protocol (CARP)
- Configuring Failover Groups for High Availability
- Feature Comparison Across Traffic Redirection Options
- 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

