AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

Securing Email with Cisco Email Security Appliance
SESA 3.0

Dauer	3 Tage
Kursstart/Status	Auf Anfrage 08:30-12:00 / 13:00-16:30
Kursort	Zürich
Kosten	CHF 3365.00
Sprache	Deutsch
Dokumentation	3.0 Offizielle Cisco Unterlagen in Englisch.

Überblick

In diesem Kurs erfahren Sie, wie Sie die Cisco Email-Security-Appliance bereitstellen und verwenden, um Schutz für Ihre E-Mail-Systeme gegen Phishing, Ransomware und anderes zu gewährleisten und die Verwaltung von E-Mail-Sicherheitsrichtlinien zu optimieren. Dieser praxisorientierte Kurs vermittelt Ihnen das Wissen und die Fähigkeiten zur Implementierung, Fehlerbehebung und Verwaltung der Cisco Email Security Appliance, einschliesslich der wichtigsten Funktionen wie erweiterter Malware-Schutz, Spam-Blockierung, Virenschutz, Ausbruchsfilterung, Verschlüsselung, Quarantäne und Schutz vor Datenverlust.

Dieser Kurs hilft Ihnen bei der Vorbereitung auf die Prüfung Securing Email with Cisco Email Security Appliance (300-720 SESA). Dies führt zu CCNP® Security und dem Certified Specialist - Email Content Security-Zertifizierungen.

Voraussetzungen

Sie verfügen bereits über die folgenden Fertigkeiten und das Wissen zu:

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

Lernziel

- Sie stellen High-Availability-E-Mail-Schutz gegen dynamische, sich schnell ändernde Bedrohungen bereit.

Zielgruppe

- Security Engineers
- Security-Administratoren
- Security-Architekten
- Operations Engineers
- Network Engineers
- Network-Administratoren
- Network- oder Security-Techniker
- Network Manager
- System Designer
- Cisco Integratoren und Partner.

Kursinhalt

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

AnyWeb Training
Cisco Certified Learning Center

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

- Describing the Cisco Email Security Appliance
  - Cisco Email Security Appliance Overview
  - Technology Use Case
  - Cisco Email Security Appliance Data Sheet
  - SMTP Overview
  - Email Pipeline Overview
  - Installation Scenarios
  - Initial Cisco Email Security Appliance Configuration
  - Centralizing Services on a Cisco Content Security Management Appliance (SMA)
  - Release Notes for AsyncOS 11.x
- Administering the Cisco Email Security Appliance
  - Distributing Administrative Tasks
  - System Administration
  - Managing and Monitoring Using the Command Line Interface (CLI)
  - Other Tasks in the GUI
  - Advanced Network Configuration
  - Using Email Security Monitor
  - Tracking Messages
  - Logging
- Controlling Sender and Recipient Domains
  - Public and Private Listeners
  - Configuring the Gateway to Receive Email
  - Host Access Table Overview
  - Recipient Access Table Overview
  - Configuring Routing and Delivery Features
- Controlling Spam with Talos SenderBase and Anti-Spam
  - SenderBase Overview
  - Anti-Spam
  - Managing Graymail
  - Protecting Against Malicious or Undesirable URLs
  - File Reputation Filtering and File Analysis
  - Bounce Verification
- Using Anti-Virus and Outbreak Filters
  - Anti-Virus Scanning Overview
  - Sophos Anti-Virus Filtering
  - McAfee Anti-Virus Filtering
  - Configuring the Appliance to Scan for Viruses
  - Outbreak Filters
  - How the Outbreak Filters Feature Works
  - Managing Outbreak Filters
- Using Mail Policies
  - Email Security Manager Overview
  - Mail Policies Overview
  - Handling Incoming and Outgoing Messages Differently
  - Matching Users to a Mail Policy
  - Message Splintering
  - Configuring Mail Policies

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

- Using Content Filters
  - Content Filters Overview
  - Content Filter Conditions
  - Content Filter Actions
  - Filter Messages Based on Content
  - Text Resources Overview
  - Using and Testing the Content Dictionaries Filter Rules
  - Understanding Text Resources
  - Text Resource Management
  - Using Text Resources
- Using Message Filters to Enforce Email Policies
  - Message Filters Overview
  - Components of a Message Filter
  - Message Filter Processing
  - Message Filter Rules
  - Message Filter Actions
  - Attachment Scanning
  - Examples of Attachment Scanning Message Filters
  - Using the CLI to Manage Message Filters
  - Message Filter Examples
  - Configuring Scan Behavior
- Preventing Data Loss
  - Overview of the Data Loss Prevention (DLP) Scanning Process
  - Setting Up Data Loss Prevention
  - Policies for Data Loss Prevention
  - Message Actions
  - Updating the DLP Engine and Content Matching Classifiers
- Using LDAP
  - Overview of LDAP
  - Working with LDAP
  - Using LDAP Queries
  - Authenticating End-Users of the Spam Quarantine
  - Configuring External LDAP Authentication for Users
  - Testing Servers and Queries
  - Using LDAP for Directory Harvest Attack Prevention
  - Spam Quarantine Alias Consolidation Queries
  - Validating Recipients Using an SMTP Server
- SMTP Session Authentication
  - Configuring AsyncOS for SMTP Authentication
  - Authenticating SMTP Sessions Using Client Certificates
  - Checking the Validity of a Client Certificate
  - Authenticating User Using LDAP Directory
  - Authenticating SMTP Connection Over Transport Layer Security (TLS) Using a Client Certificate
  - Establishing a TLS Connection from the Appliance
  - Updating a List of Revoked Certificates

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

- Email Authentication
  - Email Authentication Overview
  - Configuring DomainKeys and DomainKeys Identified MailDKIM) Signing
  - Verifying Incoming Messages Using DKIM
  - Overview of Sender Policy FrameworkSPF) and SIDF Verification
  - Domain-based Message Authentication Reporting and Conformance (DMARC) Verification
  - Forged Email Detection
- Email Encryption
  - Overview of Cisco Email Encryption
  - Encrypting Messages
  - Determining Which Messages to Encrypt
  - Inserting Encryption Headers into Messages
  - Encrypting Communication with Other Message Transfer Agents (MTAs)
  - Working with Certificates
  - Managing Lists of Certificate Authorities
  - Enabling TLS on a Listener's Host Access Table (HAT)
  - Enabling TLS and Certificate Verification on Delivery
  - Secure/Multipurpose Internet Mail Extensions (S/MIME) Security Services
- Using System Quarantines and Delivery Methods
  - Describing Quarantines
  - Spam Quarantine
  - Setting Up the Centralized Spam Quarantine
  - Using Safelists and Blocklists to Control Email Delivery Based on Sender
  - Configuring Spam Management Features for End Users
  - Managing Messages in the Spam Quarantine
  - Policy, Virus, and Outbreak Quarantines
  - Managing Policy, Virus, and Outbreak Quarantines
  - Working with Messages in Policy, Virus, or Outbreak Quarantines
  - Delivery Methods
- Centralized Management Using Clusters
  - Overview of Centralized Management Using Clusters
  - Cluster Organization
  - Creating and Joining a Cluster
  - Managing Clusters
  - Cluster Communication
  - Loading a Configuration in Clustered Appliances
  - Best Practices
- Testing and Troubleshooting
  - Debugging Mail Flow Using Test Messages: Trace
  - Using the Listener to Test the Appliance
  - Troubleshooting the Network
  - Troubleshooting the Listener
  - Troubleshooting Email Delivery
  - Troubleshooting Performance
  - Web Interface Appearance and Rendering Issues
  - Responding to Alerts
  - Troubleshooting Hardware Issues
  - Working with Technical Support

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100

Kursdetails

Garantierte Durchführung | Geplante Durchführung | Auf Anfrage | Ausgebucht, Warteliste möglich

- References
  - Model Specifications for Large Enterprises
  - Model Specifications for Midsize Enterprises and Small-to-Midsize Enterprises or Branch Offices
  - Cisco Email Security Appliance Model Specifications for Virtual Appliances
  - Packages and Licenses.

Laborübungen

- Verify and Test Cisco ESA Configuration
- Perform Basic Administration
- Advanced Malware in Attachments (Macro Detection)
- Protect Against Malicious or Undesirable URLs Beneath Shortened URLs
- Protect Against Malicious or Undesirable URLs Inside Attachments
- Intelligently Handle Unscannable Messages
- Leverage AMP Cloud Intelligence Via Pre-Classification Enhancement
- Integrate Cisco ESA with AMP Console
- Prevent Threats with Anti-Virus Protection
- Applying Content and Outbreak Filters
- Configure Attachment Scanning
- Configure Outbound Data Loss Prevention
- Integrate Cisco ESA with LDAP and Enable the LDAP Accept Query
- DomainKeys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- Forged Email Detection
- Configure the Cisco SMA for Tracking and Reporting.

Zertifizierung

Securing Email with Cisco Email Security Appliance v1.0 (SESA 300-720) ist eine 90-minütige Prüfung im Zusammenhang mit den Zertifizierungen CCNP Security und Cisco Certified Specialist - Email Content Security. Diese Prüfung testet die Kenntnisse eines Kandidaten über Cisco Email Security Appliance, einschliesslich Administration, Spam-Kontrolle und Antispam, Nachrichtenfilter, Verhinderung von Datenverlust, LDAP, E-Mail-Authentifizierung und -Verschlüsselung sowie System-Quarantänen und Zustellungsmethoden. Der Kurs "Securing Email with Cisco Email Security Appliance" hilft Kandidaten, sich auf diese Prüfung vorzubereiten.

Das Exam ist ab dem 24. Februar 2020 verfübar.

Kontakt

AnyWeb Training
Hofwiesenstrasse 350
CH-8050 Zürich-Oerlikon

training@anyweb.ch
Tel +41 58 219 1104
Fax +41 58 219 1100