Securing Your Email with Cisco IronPort C-Series (SYEPW)

Kein Kursort verfügbar

Preis CHF: 3'780.00

Preis EUR: 3'137.00

Thema/Kursziel:

Dieser Kurs vermittelt die erforderlichen Kenntnisse für die erfolgreiche Installation, Konfiguration und Administration der Cisco IronPort Email Security-Appliances. Die Teilnehmer werden tiefgehendes Know-how über die meist eingesetzten Produkt-Features erhalten mit Schwerpunkt auf:

-“Best Practices” für Konfiguration und Betrieb
-Management, Monitoring und Troubleshooting des Email-Flusses durch Cisco IronPort Email Security-Appliances
-Konfiguration von Access Control Policies
-Erstellung von Content-Filtern für die Implementierung von Corporate Email Policies
-Konfiguration von Cisco IronPort Email Security-Appliances zum Schutz gegen unerwünschten Spam und Viren
-Management der Spam-Quarantäne (C-Serie und M-Serie)
-Nutzung von Cisco IronPorts Reputation-based Services, SenderBase und Virus Outbreak Filtern zur Erhöhung der Sicherheit Ihres Email-Netzwerks
-Message Tracking und Reporting zur Dokumentation von Email Traffic Trends (C-Serie und M-Serie)
-Setzen von Delivery-Parametern für ausgehende Mail
-Integration mit einem Directory Server über LDAP
-Debugging von LDAP Integration Issues
-Nutzung von Message-Filtern zum Redirect und Ändern von Messages
-Einsatz und Debugging von Message-Filtern
-Email Authentication mit DKIM und SPF

Zielgruppen:

 Enterprise Messaging Manager und Systemadministratoren
Email Systemdesigner und Architekten
Netzwerkmanager, die für die Messaging-Implementation zuständig sind

Kursinhalt:

Module 1: Introduction & System Overview

-List IronPort Email Security Appliances
-Describe the ESA Hardware Options
-Describe the Email Pipeline Filters
-List the ESA Feature Key Options
-Describe the Operation of a Listener

Module 2: Tracking and Reporting Messages
-Perform a system installation of an M-Series
-Integrate the M-Series into the existing C-Series lab.
-Use local and Centralized Message Tracking
-Use Local and Centralized Reporting

Module 3: Controlling Sender & Recipient Domains
-Configure public and private listeners
-Configure SMTP Routes
-Use Senderbase Reputation Scores (SBRS) to manage mail
-Use Mail Debugging Tools

Module 4: Controlling Spam with SenderBase & Anti-Spam
-Adjust SBRS
-Configure Anti-Spam Settings
-Configure the IronPort Spam Quarantine
-Use the Security Management Appliance for Off Box Quarantining

Module 5: Using Anti-Virus & Virus Outbreak Filters
-Enable one or both Anti-Virus Engines
-Use one or both AV Engines in Mail Policies
-Use Virus Outbreak Filters to preemptively drop traffic and provide zero-hour protection
-Identify best practices for managing IronPort Anti-Virus

Module 6: Using Mail Policies to Direct Business Email
-Use Email Security Manager
-Create a User-Based Mail Policies
-Use Message Tracking to monitor message splintering

Module 7: Using System Quarantines and Delivery Methods
-Describe, create and manage quarantines
-Perform searches quarantine contents
-Assign Bounce Profiles
-Create Virtual Gateways

Module 8: Using Content Filters for Specific Business Needs
-Describe content scanning
-Detect password-protected / non-protected attachments
-Create weighted content matching
-Use Smart Identifiers
-Implement Matched Content Visibility
-Execute best practices when staging new filters

Module 9: Encrypting Outbound Email
-Provision with the Cisco Registered Envelope Service . Associate a content filtering rule with an “Encrypt” action . Register a CRES Envelope Recipient

Module 10: Troubleshooting
-Identify Issues
-Diagnose and Isolate Problems
-Troubleshooting tools and best practices
-Log file contents and log administration

Module 11: System Administration

-Safely upgrade software on your IronPort
-Manage users and control alerting behavior
-Manage configurations and prepare for disaster recovery Access Customer Support

Module 12: Configuring LDAP Queries

This module focuses directly on common LDAP configurations and issues. A brief overview of the Lightweight Directory Access Protocol is provided to give those new to LDAP some familiarity, but the bulk of the module assumes a basic understanding of LDAP terms and concepts. Active Directory is emphasized in a number of case studies to highlight the various installation choices. These include addressing the use of the ESA against multiple directories in a heterogeneous enterprise.

Module 13: Message Filters (Advanced Policy)

This module focuses on advanced filter options with specific emphasis on creating, troubleshooting, simplification/streamlining and regular expressions. Helpful tips and tricks for both Message and Content filters are covered. Extensive hands-on exercises are designed to give the students practice working with the Command Line Interface (CLI), as well as practical experience troubleshooting and examining logs.

Module 14: Email Authentication

This module focuses introducing Domain Keys Identified Mail and Sender Profile Framework, their role in Email Authentication and the issues of configuring it on the IronPort Appliance. Helpful examples and laboratories are provided to introduce the user to practical implementations.

Voraussetzungen:

Kenntnisse über TCP/IP-GrundlagenErfahrung mit Internet-basierendem Messaging, einschließlich SMTP, Internet- und MIME-Message-Formaten
Erfahrung mit Internet-basierendem Messaging, einschließlich SMTP, Internet- und MIME-Message-Formaten
Vertrautheit mit der Konfiguration von Devices über Command Line Interface (CLI) und Graphical User Interface (GUI)

Kursumgebung:

Der Kurs umfasst auch umfassende praktische Laborübungen mit den Advanced Features der Cisco IronPort Email Security-Appliance und versetzt die Teilnehmer dadurch in die Lage, die Cisco IronPort Email Security-Appliances für das erfolgreiche Management und Troubleshooting des gesamten eingehenden und ausgehenden Email-Verkehrs eines Unternehmens einzusetzen. Ebenso werden die Teilnehmer Advanced Internet-Email-Konzepte kennenlernen und einen Überblick über weitere Produkt-Features für spezielle kundenspezifische Konfigurationen erhalten.

Kursdokumentation:
Eine ausführliche Dokumentation (Original Cisco Unterlagen) in englischer Sprache wird den Teilnehmern abgegeben.

Dieser Kurs wird in Zusammenarbeit mit der Firma Fast Lane durchgeführt.