Securing Email with Cisco Email Security Appliance Parts 1 and 2 (SESA)

Course ID#: 1575-951-ZZ-W

Hours: 21

Course Content

Course Description:

Securing Email with Cisco Email Security Appliance (SESA) combines Parts 1 and 2 (SESA1, SESA2) into a single three day course. Students learn to use Cisco Email Security Appliances (ESA's) to manage and troubleshoot email in their networks. Attendees receive in-depth instruction on popular features, emphasizing topics listed below, learn advanced Internet email concepts and receive an overview of how to customize configurations. SESA also teaches advanced configuration and operation of the Cisco ESA (Formerly Cisco IronPort Email Security Appliance).Extensive lab exercises provide critical hands-on experience with advanced features of the ESA.

Prerequisites:

It is assumed that attendees possess the following background knowledge and skills:

- A moderate knowledge of TCP / IP fundamentals, including IP addressing and subnetting, static IP routing and DNS.
- Experience with Internet based messaging, including SMTP, Internet message formats, and MIME message format.
- Familiarity with command line interface (CLI) and graphical user interface (GUI).
- Previous experience with email security would be helpful.

Topics:

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