

## Securing Your Email with Cisco IronPort C-Series, Part I and II (SYEPW)

### Who should attend

- Enterprise messaging managers and system administrators
- Email system designers and architects
- Network managers responsible for messaging implementation

### Duration: 3 Days

### Prerequisites

- Solid knowledge of TCP/IP fundamentals, including IP addressing and sub-netting, static IP routing, DNS, and a very basic knowledge of the TCP protocol.
- Experience with Internet-based messaging, including SMTP, Internet message formats, and MIME message formatting and body parts.
- Strong familiarity both with AsyncOS command line interface (CLI) and graphical user interface (GUI) configuration of devices.

### Course Objectives

This three-day training course provides a thorough foundation for how to successfully install, configure, and administer Cisco IronPort email security appliances. Attendees receive indepth instruction on the most commonly used product features, with an emphasis on:

- How to administrate with "best practices" for configuration, operation.
- How to manage, monitor, and troubleshoot the flow of email through Cisco IronPort email security appliances.
- How to configure access control policies to eliminate threats at the perimeter, based on the identity and trustworthiness of the sender.
- How to create content filters to implement and enforce corporate email policies.
- How to configure IronPort email security appliances to detect and handle unwanted spam and viruses.
- How to manage the spam quarantine, both on the C-Series and M-Series.
- How to use Cisco IronPort's reputation-based services, SenderBase and Virus Outbreak Filters, to increase the security of your email network.
- How to use Message Tracking and Reporting to document email traffic trends, both on the C-Series and M-Series.
- How to set delivery parameters for outgoing mail. Extensive lab exercises provide attendees with skills for configuring and administering Cisco IronPort email security appliances. At the end of the course, attendees will possess a working knowledge of how to use Cisco IronPort email security appliances to successfully manage and troubleshoot email traffic entering and leaving the enterprise network.
- Integrating with a directory server via LDAP
- Debugging of LDAP integration issues
- Using message filters to redirect and modify messages
- Safe deployment and debugging of message filters
- Email Authentication with DKIM and SPF

Extensive lab exercises provide attendees with critical hands-on experience working with advanced features of the IronPort email security appliance. Attendees gain working knowledge of how to use the IronPort appliance to successfully manage and troubleshoot email traffic entering and leaving the enterprise network. Attendees will also learn about advanced Internet email concepts and receive an overview of other product features that can be used for more customized configurations.

## Course Content

### 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.