



SECURITY

Email Security with Cisco IronPort

The definitive guide to deploying and maintaining
secure email architectures with Cisco IronPort ESA

Email Security with Cisco IronPort

Chris Porter

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Email Security with Cisco IronPort

Table of Contents

Contents

Introduction

Chapter 1 Introduction to Email Security

Overview of Cisco IronPort Email Security Appliance (ESA)

AsyncOS

Security Management Appliances (SMA)

History of AsyncOS Versions

Software Features

Email Security Landscape

Email Spam

Viruses and Malware

Protecting Intellectual Property and Preventing Data Loss

Other Email Security Threats

Simple Mail Transfer Protocol (SMTP)

SMTP Commands

ESMTP Service Extensions

SMTP Message Headers and Body

Envelope Sender and Recipients

Transmitting Binary Data

Character Sets

Domain Name Service (DNS) and DNS MX Records in IPv4 and IPv6

Message Transfer Agents (MTA)

Abuse of SMTP

Summary

Chapter 2 ESA Product Basics

Table of Contents

Hardware Overview

- 2U Enterprise Models

- 1U Enterprise Models

- Selecting a Model

Basic Setup via the WUI System Setup Wizard

- Connecting to the ESA for the First Time

- Running the System Setup Wizard

- Reconnecting to the WUI

- LDAP Wizard and Next Steps

- Examining the Basic Configuration

- Next Steps

- Setup Summary

Networking Deployment Models

- Interfaces, Routing, and Virtual Gateways

- Single Versus Multinetwork Deployment

- Routing on Multinetwork Deployments

- DNS Concerns

- Firewall Rules

- Securing Network Interfaces

Security Filtering Features

- SenderBase and Reputation Filters

- IronPort Anti-Spam

- Antivirus Features

Summary

Chapter 3 ESA Email Pipeline

ESA Pipeline

- Listeners

- Host Access Table (HAT) and Reputation Filters

- Rate Limiting with Mail Flow Policies

- DNS and Envelope Checks

Table of Contents

Sender Authentication

Recipient Access Table and LDAP Accept

Recipient and Sender Manipulation

Default Domain, Domain Map, and Aliases

Masquerading

LDAP Operations

LDAP Accept

LDAP Routing and Masquerading

Groups

Work Queue and Filtering Engines

Work Queue Overview

Incoming and Outgoing Mail Policies

Message Filters

Anti-Spam Engine

Antivirus Engines

Content Filtering

Virus Outbreak Filters

DLP and Encryption

Delivery of Messages

Selecting the Delivery Interface (Virtual Gateways)

Destination Controls

Global Unsubscribe

SMTP Routes

Selecting Bounce Profiles

Handling Delivery Errors with Bounce Profiles

Final Disposition

Summary

Chapter 4 ESA Web User Interface

Overview

Connecting to the WUI

Table of Contents

WUI Tour

- Monitor Menu
- Mail Policies Menu
- Security Services Menu
- Network Menu
- System Administration Menu
- Options Menu
- Help and Support Menu

WUI with Centralized Management

- Selecting Cluster Mode
- Modify CM Options in the WUI
- Modifying Cluster Settings

Other WUI Features

- Variable WUI Appearance
- Committing Changes

Summary

Chapter 5 Command-Line Interface

Overview of the ESA Command-Line Interface

Using SSH or Telnet to Access the CLI

- PuTTY on Microsoft Windows
- Simple CLI Examples
- Getting Help
- Committing Configuration Changes

Keeping the ESA CLI Secure

- SSH Options on the ESA
- Creating and Using SSH Keys for Authentication
- Login Banners
- Restricting Access to SSH

ESA Setup Using the CLI

- Basics of Setup

Table of Contents

Next Setup Steps

Commands in Depth

Troubleshooting Example

Command Listing by Functional Area

Configuration Listing by Functional Area

Batch Commands

Hidden/Undocumented Commands

Summary

Chapter 6 Additional Management Services

The Need for Additional Protocol Support

Simple Network Management Protocol (SNMP)

Enabling SNMP

SNMP Security

Enterprise MIBs

Other MIBs

Monitoring Recommendations

Working with the ESA Filesystem

ESA Logging

ESA Subsystem Logs

Administrative and Auditing Logs

Email Activity Logs

Debugging Logs

Archive Logs

Creating a Log Subscription

Logging Recommendations

Transferring Logs for Permanent Storage

Understanding IronPort Text Mail Logs

Message Events

Lifecycle of a Message in the Log

Tracing Message History

Table of Contents

- Parsing Message Events
- A Practical Example of Log Parsing
- Using Custom Log Entries

Summary

Chapter 7 Directories and Policies

Directory Integration

- The Need for Directory Integration
- Security Concerns

Brief LDAP Overview

LDAP Setup on ESA

- Advanced Profile Settings
- Basic Query Types
- Recipient Validation with LDAP
- Recipient Routing with LDAP
- Sender Masquerading
- Group Queries
- Authentication Queries
- AD Specifics
- Testing LDAP Queries
- Advanced LDAP Queries
- Troubleshooting LDAP

Incoming and Outgoing Mail Policies

- Group-Based Policies
- Group Matches in Filters

Other LDAP Techniques

- Using Group Queries for Routing
- Using Group Queries for Recipient and Sender Validation

Summary

Chapter 8 Security Filtering

Table of Contents

Overview

The Criminal Ecosystem

Reputation Filters and SenderBase Reputation Scores

- Enabling Reputation Filters

- Reputation Scores

- Connection Actions

- HAT Policy Recommendations

IronPort Anti-Spam (IPAS)

- Enabling IPAS

- IPAS Verdicts

- IPAS Actions

- Content Filters and IPAS

Recommended Anti-Spam Settings

- Spam Thresholds

- Actions for the Bold

- Actions for the Middle-of-the-Road

- Actions for the Conservative

- Outgoing Anti-Spam Scanning

Sophos and McAfee Antivirus (AV)

- Enabling AV

- AV Verdicts

- AV Actions

- AV Notifications

- Content Filters and AV

IronPort Outbreak Filters (OF)

- Enabling OF

- OF Verdicts

- OF Actions

- Message Modification

- Content Filters and OF

Table of Contents

Recommended AV Settings

- Incoming AV Recommendations

- Outgoing AV Recommendations

Using Content Filters for Security

- Attachment Conditions and Actions

- Filtering Bad Senders

- Filtering Subject or Body

Summary

Chapter 9 Automating Tasks

Administering ESA from Outside Servers

CLI Automation Examples

- SSH Clients

- Expect

- Perl

- CLI Automation from Microsoft Windows Servers

WUI Automation Examples

Polling Data from the ESA

- Retrieving XML Data Pages

- Using XML Export for Monitoring

Pushing Data to the ESA and Making Configuration Changes

- Changing Configuration Settings Using the CLI

- Committing Changes Using the CLI

- Changing Configuration Settings Using the WUI

- Committing Changes Using the WUI

Retrieving Reporting Data from the WUI

- Data Export URLs

- Other Data Export Topics

- Example Script

Summary

Table of Contents

Chapter 10 Configuration Files

- ESA and the XML Configuration Format

- Configuration File Structure

- Importing and Exporting Configuration Files

 - Exporting

 - Importing

- Editing Configuration Files

 - Duplicating a Configuration

 - Partial Configuration Files

- Automating Configuration File Backup

- Configuration Backup via CLI

- Configuration Backup via WUI

- Configuration Files in Centralized Management Clusters

- Summary

Chapter 11 Message and Content Filters

- Filtering Email Messages with Custom Rules

 - Message Filters Versus Content Filters

- Filter Conditions

 - Conditions That Test Message Data

 - Operating on Message Metadata

 - Attachment Conditions

 - System State Conditions

 - Miscellaneous Filter Conditions

- Filter Actions

 - Changing Message Data

 - Altering Message Body

 - Affecting Message Delivery

 - Altering Message Processing

 - Miscellaneous Filter Actions

Table of Contents

Action Variables

Regular Expressions in Filters

Dictionaries

Notification Templates

Smart Identifiers

- Using Smart Identifiers

- Smart Identifier Best Practices

Content Filter and Mail Policy Interaction

Filter Performance Considerations

- Improving Filter Performance

Filter Recipes

- Dropping Messages

- Basic Message Attribute Filters

- Body and Attachment Scanning

- Complex Combinatorial Logic with Content Filters

- Routing Messages Using Filters

- Integration with External SMTP Systems

- Interacting with Security Filters

- Reinjection of Messages

Summary

Chapter 12 Advanced Networking

ESA with Multiple IP Interfaces

- Multihomed Deployments

- Virtual Gateways

- Adding New Interfaces and Groups

- Using Virtual Gateways for Email Delivery

- Virtual Gateways and Listeners

Multiple Listeners

- Separating Incoming and Outgoing Mail

Table of Contents

Multiple Outgoing Mail Listeners

Separate Public MX from Submission

ESA and Virtual LANs

Other Advanced Configurations

Static Routing

Transport Layer Security

Split DNS

Load Balancers and Direct Server Return (DSR)

Summary

Chapter 13 Multiple Device Deployments

General Deployment Guidelines

Email Availability with Multiple ESAs

Load-Balancing Strategies

SMTP MX Records

Multitier Architectures

Two-Tiered Architectures

Three-Tiered Architectures

Functional Grouping

Architectures with Mixed MTA Products

Integration with External Systems

External Email Encryption

External Data Loss Prevention (DLP) Servers

Email Archiving Servers

Introducing, Replacing, or Upgrading ESA in Production

Adding the First ESA to the Environment

Replacing an ESA for Upgrade

Management of Multiple Appliances

Centralized Management Overview

Creating a CM Cluster

Table of Contents

- Joining an Existing CM Cluster
- Creating and Managing CM Groups
- Using CM in the WUI
- Using CM in the CLI
- Centralized Management Limitations and Recommendations

Summary

Chapter 14 Recommended Configuration

Best Practices

- Redundancy and Capacity
- Securing the Appliance

Security Filtering

- HAT Policy Settings
- Whitelisting and Blacklisting
- Spam Quarantining
- Automated Notifications

Being a Good Sender

- Being Rate Limited
- Outbound Sending Practices
- Handling Bounces
- Variable Envelope Return Path
- DNS and Sender Authentication
- Dealing with Blacklisting
- Compromised Internal Sources

Bounce Verification

Recommendations for Specific Environments

- Small and Medium Organizations
- Large or Complex Organizations
- Service Providers
- Higher Education
- Email Front End to Complex Internal Organizations

Table of Contents

Summary

Chapter 15 Advanced Topics

Recent Developments

Authentication Standards

Path-Authentication Standards: SPF and SIDF

DKIM and SPF Recommendations

Regulatory Compliance

General Concepts

Data Loss Prevention (DLP)

Enabling Data Loss Prevention Policies

Classifiers and Entities

Customizing Policies

Summary

Index