



Preface **Ixiii**

Conventions **Ixiii**

Obtain Documentation and Submit a Service Request **Ixiv**

PART 1

The Basics of Using Security Manager

CHAPTER 1

Getting Started with Security Manager **1-1**

Product Overview **1-1**

Primary Benefits of Cisco Security Manager **1-2**

Security Manager Policy Feature Sets **1-4**

Security Manager Applications Overview **1-6**

Device Monitoring Overview **1-7**

IPv6 Support in Security Manager **1-8**

 Configuring IPv6 on Security Manager Server **1-9**

 Configuring IPv6 Policies **1-9**

 Policy Object Changes in Security Manager 4.4 **1-10**

Logging In to and Exiting Security Manager **1-11**

 Understanding User Permissions **1-11**

 Logging In to the Cisco Security Management Suite Server **1-12**

 Logging In to and Exiting the Security Manager Client **1-12**

Using Configuration Manager - Overview **1-14**

 Configuration Manager Overview **1-14**

 Device View Overview **1-15**

 Policy View Overview **1-16**

 Map View Overview **1-18**

 Task Flow for Configuring Security Policies **1-19**

 Policy and Policy Object Overview **1-20**

 Workflow and Activities Overview **1-20**

 Working in Workflow Mode **1-21**

 Working in Non-Workflow Mode **1-22**

 Comparing Workflow Modes **1-22**

Using the JumpStart to Learn About Security Manager **1-24**

Completing the Initial Security Manager Configuration **1-25**

Configuring an SMTP Server and Default Addresses for E-Mail Notifications	1-27
Changing Workflow Modes	1-28
Understanding Basic Security Manager Interface Features	1-29
Menu Bar Reference for Configuration Manager	1-29
File Menu (Configuration Manager)	1-30
Edit Menu (Configuration Manager)	1-31
View Menu (Configuration Manager)	1-31
Policy Menu (Configuration Manager)	1-32
Map Menu (Configuration Manager)	1-33
Manage Menu (Configuration Manager)	1-34
Tools Menu (Configuration Manager)	1-34
Activities Menu (Configuration Manager)	1-36
Tickets Menu (Configuration Manager)	1-36
Launch Menu (Configuration Manager)	1-37
Help Menu (Configuration Manager)	1-38
Toolbar Reference (Configuration Manager)	1-39
Using Global Search	1-42
Using Selectors	1-45
Filtering Items in Selectors	1-45
Create Filter Dialog Box	1-46
Using Wizards	1-47
Using Tables	1-48
Filtering Tables	1-48
Table Columns and Column Heading Features	1-49
Using Text Fields	1-49
Understanding ASCII Limitations for Text	1-50
Finding Text in Text Boxes	1-50
Navigating Within Text Boxes	1-50
Selecting or Specifying a File or Directory in Security Manager	1-50
Troubleshooting User Interface Problems	1-51
Accessing Online Help	1-52

CHAPTER 2

Preparing Devices for Management 2-1

Understanding Device Communication Requirements	2-1
Setting Up SSL (HTTPS)	2-3
Setting Up SSL (HTTPS) on PIX Firewall, ASA and FWSM Devices	2-3
Setting Up SSL on Cisco IOS Routers	2-4
Setting Up SSH	2-5
Critical Line-Ending Conventions for SSH	2-5

Testing Authentication	2-6
Setting Up SSH on Cisco IOS Routers, Catalyst Switches, and Catalyst 6500/7600 devices	2-6
Preventing Non-SSH Connections (Optional)	2-7
Setting Up AUS or Configuration Engine	2-8
Setting Up AUS on PIX Firewall and ASA Devices	2-8
Configuring Licenses on Cisco ASA Devices	2-9
Configuring Licenses on Cisco IOS Devices	2-10
Initializing IPS Devices	2-10

CHAPTER 3**Managing the Device Inventory 3-1**

Understanding the Device Inventory	3-1
Understanding the Device View	3-1
Understanding Device Names and What Is Considered a Device	3-3
Understanding Device Credentials	3-4
Understanding Device Properties	3-6
Adding Devices to the Device Inventory	3-6
Working with Generically Supported Devices	3-8
Working with Device Clusters	3-9
Adding Devices from the Network	3-12
Device Information Page – Add Device from Network	3-14
Service Module Credentials Dialog Box	3-19
IPS Module Discovery Dialog Box	3-20
Adding Devices from Configuration Files	3-22
Device Information Page—Configuration File	3-23
Adding Devices by Manual Definition	3-26
Device Information Page—New Device	3-27
Adding Devices from an Inventory File	3-31
Device Information Page—Add Device from File	3-33
Working with the Device Inventory	3-36
Adding, Editing, or Deleting Auto Update Servers or Configuration Engines	3-36
Server Properties Dialog Box	3-38
Available Servers Dialog Box	3-39
Adding or Changing Interface Modules	3-40
Viewing or Changing Device Properties	3-40
Device Properties: General Page	3-41
Device Credentials Page	3-45
Device Groups Page	3-49
Cluster Information Page	3-50
Policy Object Override Pages	3-52

- Changing Critical Device Properties 3-52
 - Image Version Changes That Do Not Change the Feature Set in Security Manager 3-53
 - Changes That Change the Feature Set in Security Manager 3-54
- Showing Device Containment 3-56
- Cloning a Device 3-56
- Deleting Devices from the Security Manager Inventory 3-58
 - Device Delete Validation Dialog Box 3-59
- Working with Device Groups 3-59
 - Understanding Device Grouping 3-60
 - Edit Device Groups Dialog Box 3-61
 - Creating Device Group Types 3-62
 - Creating Device Groups 3-62
 - Deleting Device Groups or Group Types 3-63
 - Adding Devices to or Removing Them From Device Groups 3-63
- Working with Device Status View 3-64

CHAPTER 4

Managing Activities 4-1

- Understanding Activities 4-1
 - Benefits of Activities 4-2
 - Activity Approval 4-3
 - Activities and Locking 4-3
 - Activities and Multiple Users 4-4
 - Understanding Activity/Ticket States 4-4
- Working with Activities/Tickets 4-7
 - Accessing Activity Functions in Workflow Mode 4-8
 - Accessing Ticket Functions in Non-Workflow Mode 4-9
 - Activity/Ticket Manager Window 4-10
 - Creating an Activity/Ticket 4-14
 - 2019 Responding to the Activity/Ticket Required Dialog Box 4-14
 - Opening an Activity/Ticket 4-15
 - Closing an Activity/Ticket 4-16
 - Viewing Change Reports 4-16
 - Selecting a Change Report in Non-Workflow Mode with Ticket Management Disabled 4-18
 - Validating an Activity/Ticket 4-18
 - Submitting an Activity for Approval (Workflow Mode with Activity Approver) 4-20
 - Approving or Rejecting an Activity (Workflow Mode) 4-21
 - Discarding an Activity/Ticket 4-22
 - Viewing Activity/Ticket Status and History 4-23

CHAPTER 5

Managing Policies 5-1

Understanding Policies	5-1
Settings-Based Policies vs. Rule-Based Policies	5-2
Service Policies vs. Platform-Specific Policies	5-2
Local Policies vs. Shared Policies	5-3
Understanding Rule Inheritance	5-4
Inheritance vs. Assignment	5-6
Policy Management and Objects	5-7
Understanding Policy Locking	5-8
Understanding Locking and Policies	5-9
Understanding Locking and VPN Topologies	5-10
Understanding Locking and Objects	5-10
Customizing Policy Management for Routers and Firewall Devices	5-11
Discovering Policies	5-12
Discovering Policies on Devices Already in Security Manager	5-15
Create Discovery Task and Bulk Rediscovery Dialog Boxes	5-18
Viewing Policy Discovery Task Status	5-22
Discovery Status Dialog Box	5-23
Policy Discovery Status Page	5-25
Frequently Asked Questions about Policy Discovery	5-27
Managing Policies in Device View and the Site-to-Site VPN Manager	5-30
Policy Status Icons	5-30
Performing Basic Policy Management	5-31
Configuring Local Policies in Device View	5-31
Copying Policies Between Devices	5-33
Unassigning a Policy	5-36
Working with Shared Policies in Device View or the Site-to-Site VPN Manager	5-37
Using the Policy Banner	5-38
Policy Shortcut Menu Commands in Device View and the Site-to-Site VPN Manager	5-40
Sharing a Local Policy	5-41
Sharing Multiple Policies of a Selected Device	5-42
Unsharing a Policy	5-43
Assigning a Shared Policy to a Device or VPN Topology	5-44
Adding Local Rules to a Shared Policy	5-45
Inheriting or Uninheriting Rules	5-47
Cloning (Copying) a Shared Policy	5-47
Renaming a Shared Policy	5-48
Modifying Shared Policy Definitions in Device View or the Site-to-Site VPN Manager	5-49
Modifying Shared Policy Assignments in Device View or the Site-to-Site VPN Manager	5-49

- Managing Shared Policies in Policy View 5-50
 - Policy View Selectors 5-52
 - Policy View—Shared Policy Selector Options 5-53
 - Creating a New Shared Policy 5-54
 - Modifying Policy Assignments in Policy View 5-54
 - Deleting a Shared Policy 5-56
- Managing Policy Bundles 5-57
 - Creating a New Policy Bundle 5-57
 - Cloning a Policy Bundle 5-58
 - Renaming a Policy Bundle 5-58
 - Assigning Policy Bundles to Devices 5-59

CHAPTER 6

Managing Policy Objects 6-1

- Selecting Objects for Policies 6-2
- Policy Object Manager 6-4
 - Policy Object Manager: Undocking and Docking 6-8
 - Policy Object Manager Shortcut Menu 6-8
- Working with Policy Objects—Basic Procedures 6-9
 - Creating Policy Objects 6-9
 - Editing Objects 6-12
 - Using Category Objects 6-13
 - Cloning (Duplicating) Objects 6-14
 - Viewing Object Details 6-14
 - Generating Object Usage Reports 6-15
 - Deleting Objects 6-16
 - Managing Object Overrides 6-17
 - Understanding Policy Object Overrides for Individual Devices 6-18
 - Allowing a Policy Object to Be Overridden 6-18
 - Creating or Editing Object Overrides for a Single Device 6-19
 - Creating or Editing Object Overrides for Multiple Devices At A Time 6-19
 - Deleting Device-Level Object Overrides 6-21
 - Overridable Objects in Security Manager 6-22
 - Importing and Exporting Policy Objects 6-23
- Understanding AAA Server and Server Group Objects 6-27
 - Supported AAA Server Types 6-28
 - Additional AAA Support on ASA, PIX, and FWSM Devices 6-28
 - Predefined AAA Authentication Server Groups 6-30
 - Default AAA Server Groups and IOS Devices 6-31
 - Creating AAA Server Objects 6-32

Add or Edit AAA Server Dialog Box	6-33
AAA Server Dialog Box—RADIUS Settings	6-35
AAA Server Dialog Box—TACACS+ Settings	6-38
AAA Server Dialog Box—Kerberos Settings	6-39
AAA Server Dialog Box—LDAP Settings	6-40
AAA Server Dialog Box—NT Settings	6-43
AAA Server Dialog Box—SDI Settings	6-43
AAA Server Dialog Box—HTTP-FORM Settings	6-44
Add and Edit LDAP Attribute Map Dialog Boxes	6-46
Add and Edit LDAP Attribute Map Value Dialog Boxes	6-47
Add and Edit Map Value Dialog Boxes	6-47
Creating AAA Server Group Objects	6-48
AAA Server Group Dialog Box	6-49
Creating Access Control List Objects	6-53
Creating Extended Access Control List Objects	6-54
Creating Standard Access Control List Objects	6-56
Creating Web Access Control List Objects	6-57
Creating Unified Access Control List Objects	6-58
Add or Edit Access List Dialog Boxes	6-59
Add and Edit Extended Access Control Entry Dialog Boxes	6-61
Add and Edit Standard Access Control Entry Dialog Boxes	6-64
Add and Edit Web Access Control Entry Dialog Boxes	6-65
Add and Edit Unified Access Control Entry Dialog Boxes	6-67
Configuring Time Range Objects	6-71
Recurring Ranges Dialog Box	6-72
Understanding Interface Role Objects	6-73
Creating Interface Role Objects	6-74
Interface Role Dialog Box	6-75
Specifying Interfaces During Policy Definition	6-76
Using Interface Roles When a Single Interface Specification is Allowed	6-77
Handling Name Conflicts between Interfaces and Interface Roles	6-78
Understanding Map Objects	6-78
Understanding Networks/Hosts Objects	6-80
Contiguous and Discontiguous Network Masks for IPv4 Addresses	6-81
Creating Networks/Hosts Objects	6-82
Add or Edit Network/Host Dialog Box	6-83
Using Unspecified Networks/Hosts Objects	6-86
Specifying IP Addresses During Policy Definition	6-87
VM Attribute Policies	6-89

- Communication between the VM attribute agent and vCenter 6-89
- Attribute Agent States 6-90
- Guidelines for Configuring vCenter Virtual Machines 6-90
- Configuring VM Attribute Policies 6-91
- Understanding Pool Objects 6-92
 - Add or Edit IPv4 Pool Dialog Box 6-92
 - Add or Edit IPv6 Pool Dialog Box 6-93
 - Add or Edit MAC Address Pool Dialog Box 6-94
 - Add or Edit NET Pool Object Dialog Box 6-95
 - Add or Edit DHCPv6 Pool Dialog Box 6-96
- Configuring SAML Identity Provider 6-98
 - Adding or Editing SAML Identity Provider 6-98
- Understanding and Specifying Services and Service and Port List Objects 6-100
 - Configuring Port List Objects 6-102
 - Configuring Service Objects 6-103
- How Policy Objects are Provisioned as Object Groups 6-106
 - How Network/Host, Port List, and Service Objects are Named When Provisioned As Object Groups 6-107
 - How Service Objects are Provisioned as Object Groups 6-108

CHAPTER 7

Managing FlexConfigs 7-1

- Understanding FlexConfig Policies and Policy Objects 7-2
 - Using CLI Commands in FlexConfig Policy Objects 7-2
 - Using Scripting Language Instructions 7-3
 - Scripting Language Example 1: Looping 7-3
 - Scripting Language Example 2: Looping with Two-Dimensional Arrays 7-3
 - Example 3: Looping with If/Else Statements 7-4
- Understanding FlexConfig Object Variables 7-5
 - Example of FlexConfig Policy Object Variables 7-6
 - FlexConfig System Variables 7-7
- Predefined FlexConfig Policy Objects 7-19
- Configuring FlexConfig Policies and Policy Objects 7-25
 - A FlexConfig Creation Scenario 7-25
 - Creating FlexConfig Policy Objects 7-28
 - Add or Edit FlexConfig Dialog Box 7-30
 - Create Text Object Dialog Box 7-32
 - Add or Edit Text Object Dialog Box 7-32
 - FlexConfig Undefined Variables Dialog Box 7-33
 - Property Selector Dialog Box 7-34

Editing FlexConfig Policies	7-35
FlexConfig Policy Page	7-36
Values Assignment Dialog Box	7-37
FlexConfig Preview Dialog Box	7-38
Troubleshooting FlexConfigs	7-38

CHAPTER 8**Managing Deployment 8-1**

Understanding Deployment	8-1
Overview of the Deployment Process	8-1
Deployment in Non-Workflow Mode	8-3
Deployment Task Flow in Non-Workflow Mode	8-3
Job States in Non-Workflow Mode	8-4
Deployment in Workflow Mode	8-5
Deployment Task Flow in Workflow Mode	8-5
Job States in Workflow Mode	8-6
Deployment Job Approval	8-7
Deployment Jobs and Multiple Users	8-8
Including Devices in Deployment Jobs or Schedules	8-8
Understanding Deployment Methods	8-8
Deploying Directly to a Device	8-9
Deploying to a Device through an Intermediate Server	8-10
Deploying to a File	8-11
Understanding How Out-of-Band Changes are Handled	8-12
Handling Device OS Version Mismatches	8-13
Overview of the Deployment Manager and Configuration Archive	8-15
Understanding What You Can Do with the Deployment Manager	8-16
Deployment Manager Window	8-16
Deployment Workflow Commentary Dialog Box	8-20
Deployment Schedules Tab, Deployment Manager	8-21
Configuration Archive Window	8-23
Working with Deployment and the Configuration Archive	8-25
Viewing Deployment Status and History for Jobs and Schedules	8-26
Tips for Successful Deployment Jobs	8-27
Deploying Configurations in Non-Workflow Mode	8-28
Edit Deploy Method Dialog Box	8-30
Warning - Partial VPN Deployment Dialog Box	8-31
Deployment Status Details Dialog Box	8-32
Deploying Configurations in Workflow Mode	8-34
Creating and Editing Deployment Jobs	8-35

- Submitting Deployment Jobs 8-38
- Approving and Rejecting Deployment Jobs 8-39
- Deploying a Deployment Job in Workflow Mode 8-39
- Discarding Deployment Jobs 8-41
- Deploying Configurations Using an Auto Update Server or CNS Configuration Engine 8-41
- Deploying Configurations to a Token Management Server 8-43
- Previewing Configurations 8-44
- Detecting and Analyzing Out of Band Changes 8-45
 - Exceptions to Out of Band Change Detection 8-47
 - OOB (Out of Band) Changes Dialog Box 8-48
 - OOB Re-sync. Tool 8-50
- Redeploying Configurations to Devices 8-53
- Aborting Deployment Jobs 8-55
- Creating or Editing Deployment Schedules 8-55
 - Schedule Dialog Box 8-56
 - Add Other Devices Dialog Box 8-58
- Suspending or Resuming Deployment Schedules 8-58
- Adding Configuration Versions from a Device to the Configuration Archive 8-59
- Viewing and Comparing Archived Configuration Versions 8-59
 - Configuration Version Viewer 8-60
- Viewing Deployment Transcripts 8-62
- Rolling Back Configurations 8-63
 - Understanding Configuration Rollback 8-63
 - Understanding Rollback for Devices in Multiple Context Mode 8-64
 - Understanding Rollback for Failover Devices 8-65
 - Understanding Rollback for Catalyst 6500/7600 Devices 8-65
 - Understanding Rollback for IPS and IOS IPS 8-66
 - Commands that Can Cause Conflicts after Rollback 8-67
 - Commands to Recover from Failover Misconfiguration after Rollback 8-68
 - Rolling Back Configurations to Devices Using the Deployment Manager 8-69
 - Using Rollback to Deploy Archived Configurations 8-70
 - Performing Rollback When Deploying to a File 8-71

CHAPTER 9

Troubleshooting Device Communication and Deployment 9-1

- Testing Device Connectivity 9-1
 - Device Connectivity Test Dialog Box 9-3
- Managing Device Communication Settings and Certificates 9-4
 - Multiple Certificate Authentication Support 9-4
 - Manually Adding SSL Certificates for Devices that Use HTTPS Communications 9-5

Security Certificate Rejected When Discovering Device	9-6
Invalid Certificate Error During Device Discovery	9-7
Troubleshooting SSH Connection Problems	9-7
Troubleshooting Device Communication Failures	9-8
Resolving Red X Marks in the Device Selector	9-9
Troubleshooting Deployment	9-9
Changing How Security Manager Responds to Device Messages	9-10
Memory Violation Deployment Errors for ASA 8.3+ Devices	9-12
Error While Attempting to Remove Unreferenced Object	9-12
Security Manager Unable to Communicate With Device After Deployment	9-12
Updating VPNs That Include Routing Processes	9-13
Mixing Deployment Methods with Router and VPN Policies	9-14
Deployment Failures for Routers	9-14
Deployment Failures for Catalyst Switches and Service Modules	9-16
Changing How Security Manager Deploys Configurations to Multiple-Context FWSM	9-17
Deployment Failures to Devices Managed by AUS	9-18
Troubleshooting the Setup of Configuration Engine-Managed Devices	9-18

CHAPTER 10**Managing the Security Manager Server 10-1**

Overview of Security Manager Server Management and Administration	10-1
Managing a Cluster of Security Manager Servers	10-2
Overview of Security Manager Server Cluster Management	10-2
Splitting a Security Manager Server	10-3
Synchronizing Shared Policies Among Security Manager Servers	10-5
Exporting the Device Inventory	10-6
Exporting the Device Inventory from the Security Manager Client	10-6
Supported CSV Formats for Inventory Import/Export	10-9
Exporting the Device Inventory from the Command Line	10-10
Exporting Shared Policies	10-12
Importing Policies or Devices	10-13
Installing Security Manager License Files	10-16
Certificate Trust Management	10-18
Working with Audit Reports	10-19
Understanding Audit Reports	10-19
Generating the Audit Report	10-20
Using the Audit Report Window	10-21
Purging Audit Log Entries	10-23
Taking Over Another User's Work	10-23
Changing Passwords for the Admin or Other Users	10-24

Backing up and Restoring the Security Manager Database	10-24
Backing Up the Server Database	10-25
Restoring the Server Database	10-27
Generating Data for the Cisco Technical Assistance Center	10-28
Creating Diagnostics Files for the Cisco Technical Assistance Center	10-28
Generating Deployment or Discovery Status Reports	10-30
Generating a Partial Database Backup for the Cisco Technical Assistance Center	10-30

CHAPTER 11

Configuring Security Manager Administrative Settings 11-1

API Settings Page	11-2
AutoLink Settings Page	11-3
ACL Hit Count Settings Page	11-3
CCO Settings Page	11-4
Configuration Archive Page	11-6
CS-MARS Page	11-7
New or Edit CS-MARS Device Dialog Box	11-8
CSM Mobile Page	11-9
Customize Desktop Page	11-10
Debug Options Page	11-11
Deployment Page	11-13
Device Communication Page	11-21
Add Certificate Dialog Box	11-24
Device Groups Page	11-24
Discovery Page	11-25
Event Management Page	11-27
Troubleshooting Syslog Relay Servers	11-33
Device Management via IP	11-33
CPU Throttling Policy Dialog Box	11-33
Syslog Relay Statistics Dialog Box	11-35
Health and Performance Monitor Page	11-36
Report Manager Page	11-38
Identity Settings Page	11-38
Image Manager Page	11-41
IP Intelligence Settings Page	11-41
Eventing Notification Settings Page	11-45
IPS Updates Page	11-47
Edit Update Server Settings Dialog Box	11-52

Edit Auto Update Settings Dialog Box	11-54
Edit Signature Download Filter Settings Dialog Box	11-55
ISE Settings Page	11-56
Licensing Page	11-57
CSM Tab, Licensing Page	11-57
IPS Tab, Licensing Page	11-58
Verifying IPS Devices for License Update or Redeployment	11-60
Selecting IPS License Files	11-61
License Update Status Details Dialog Box	11-62
Logs Page	11-62
Policy Management Page	11-64
Policy Objects Page	11-66
Process Monitoring Settings Page	11-67
Single Sign-on Configuration Page	11-68
Rule Expiration Page	11-69
Server Security Page	11-70
Take Over User Session Page	11-71
Ticket Management Page	11-72
Token Management Page	11-73
VPN Policy Defaults Page	11-74
Workflow Page	11-75
Wall Settings Page	11-77

PART 2**Firewall Services and NAT****CHAPTER 12****Introduction to Firewall Services 12-1**

Overview of Firewall Services	12-1
Understanding the Processing Order of Firewall Rules	12-2
Understanding How NAT Affects Firewall Rules	12-3
ACL Names Preserved by Security Manager	12-4
ACL Naming Conventions	12-5
Resolving User Defined ACL Policy Naming Conflicts	12-6
Resolving ACL Name Conflicts Between Policies	12-7
Managing Your Rules Tables	12-7
Using Rules Tables	12-8
Adding and Removing Rules	12-9
Editing Rules	12-10

Adding or Editing Address Cells in Rules Tables	12-11
Adding or Editing User Cells in Rules Tables	12-12
Adding or Editing Services Cells in Rules Tables	12-13
Adding or Editing Interfaces or Zones Cells in Rules Tables	12-13
Editing Category Cells in Rules Tables	12-14
Editing Description Cells in Rules Tables	12-14
Showing the Contents of Cells in Rules Tables	12-14
Finding and Replacing Items in Rules Tables	12-16
Find and Replace Dialog Box	12-17
Moving Rules and the Importance of Rule Order	12-19
Enabling and Disabling Rules	12-20
Using Sections to Organize Rules Tables	12-20
Add and Edit Rule Section Dialog Boxes	12-22
Combining Rules	12-22
Combine Rules Selection Summary Dialog Box	12-24
Interpreting Rule Combiner Results	12-25
Example Rule Combiner Results	12-27
Converting IPv4 Rules to Unified Rules	12-28
Generating Policy Query Reports	12-28
Querying Device or Policy Dialog Box	12-29
Interpreting Policy Query Results	12-32
Example Policy Query Result	12-34
Optimizing Network Object Groups When Deploying Firewall Rules	12-35
Expanding Object Groups During Discovery	12-35

CHAPTER 13

Managing Identity-Aware Firewall Policies	13-1
Overview of Identity-Aware Firewall Policies	13-1
User Identity Acquisition	13-2
Requirements for Identity-Aware Firewall Policies	13-3
Configuring the Firewall to Provide Identity-Aware Services	13-7
Configuring Identity-Aware Firewall Policies	13-7
Enabling Identity-Aware Firewall Services	13-8
Identifying Active Directory Servers and Agents	13-8
Configuring Identity Options	13-15
Creating Identity User Group Objects	13-19
Selecting Identity Users in Policies	13-21
Configuring Identity-Based Firewall Rules	13-21
Configuring Cut-Through Proxy	13-23
Collecting User Statistics	13-25

Filtering VPN Traffic with Identity-Based Rules	13-26
Monitoring Identity Firewall Policies	13-27

CHAPTER 14**Managing TrustSec Firewall Policies 14-1**

Overview of TrustSec Firewall Policies	14-1
Understanding SGT and SXP Support in Cisco TrustSec	14-2
Roles in the Cisco TrustSec Solution	14-3
Security Group Policy Enforcement	14-3
About Speaker and Listener Roles	14-6
Prerequisites for Integrating an ASA with Cisco TrustSec	14-6
Configuring TrustSec Firewall Policies	14-7
Configuring Cisco TrustSec Services	14-8
Configuring Security Exchange Protocol (SXP) Settings	14-8
Defining SXP Connection Peers	14-12
Creating Security Group Objects	14-14
Selecting Security Groups in Policies	14-16
Configuring TrustSec-Based Firewall Rules	14-17
Monitoring TrustSec Firewall Policies	14-17

CHAPTER 15**Managing Firewall AAA Rules 15-1**

Understanding AAA Rules	15-1
Understanding How Users Authenticate	15-2
Configuring AAA Rules for ASA, PIX, and FWSM Devices	15-4
Configuring AAA Rules for IOS Devices	15-7
AAA Rules Page	15-10
Add and Edit AAA Rule Dialog Boxes	15-13
Edit AAA Option Dialog Box	15-19
AuthProxy Dialog Box	15-19
Edit Server Group Dialog Box	15-19
AAA Firewall Settings Policies	15-20
AAA Firewall Settings Page, Advanced Setting Tab	15-20
Interactive Authentication Configuration Dialog Box	15-24
Clear Connection Configuration Dialog Box	15-25
AAA Firewall Page, MAC-Exempt List Tab	15-26
Firewall AAA MAC Exempt Setting Dialog Box	15-27
AAA Page	15-28
Firewall AAA IOS Timeout Value Setting	15-30

CHAPTER 16

Managing Firewall Access Rules 16-1

- Understanding Access Rules 16-1
 - Understanding Global Access Rules 16-3
 - Understanding Device Specific Access Rule Behavior 16-4
 - Understanding Access Rule Address Requirements and How Rules Are Deployed 16-5
- Configuring Access Rules 16-7
 - Access Rules Page 16-10
 - Add and Edit Access Rule Dialog Boxes 16-14
 - Advanced and Edit Options Dialog Boxes 16-17
 - Hit Count Selection Summary Dialog Box 16-20
- Configuring Expiration Dates for Access Rules 16-22
- Configuring Settings for Access Control 16-23
 - Access Control Settings Page 16-24
 - Firewall ACL Setting Dialog Box 16-26
- Using Automatic Conflict Detection 16-28
 - Understanding Automatic Conflict Detection 16-28
 - Understanding the Automatic Conflict Detection User Interface 16-30
 - Resolving Conflicts 16-34
- Viewing Hit Count Details 16-36
 - Sample Hit Count Details Window 16-38
- Importing Rules 16-40
 - Import Rules Wizard—Enter Parameters Page 16-41
 - Import Rules Wizard—Status Page 16-42
 - Import Rules Wizard—Preview Page 16-43
 - Examples of Imported Rules 16-44
- Optimizing Access Rules Automatically During Deployment 16-46
- Customizing defaults in the Add Access Rule dialog 16-48

CHAPTER 17

Managing Firewall Inspection Rules 17-1

- Understanding Inspection Rules 17-2
 - Choosing the Interfaces for Inspection Rules 17-2
 - Selecting Which Protocols To Inspect 17-3
 - Understanding Access Rule Requirements for Inspection Rules 17-4
 - Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices 17-5
- Configuring Inspection Rules 17-5
- Inspection Rules Page 17-8
 - Add or Edit Inspect/Application FW Rule Wizard 17-11
 - Add or Edit Inspect/Application FW Rule Wizard, Step 2 17-13

Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page	17-17
Configure DNS Dialog Box	17-19
Configure SMTP Dialog Box	17-20
Configure ESMTP Dialog Box	17-20
Configure Fragments Dialog Box	17-20
Configure IMAP or POP3 Dialog Boxes	17-21
Configure RPC Dialog Box	17-21
Custom Protocol Dialog Box	17-22
Configure Dialog Box	17-22
Configuring Protocols and Maps for Inspection	17-22
Configuring Class Maps for Inspection Policies	17-28
Configuring DCE/RPC Maps	17-29
DCE/RPC Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes	17-31
Configuring DNS Maps	17-32
DNS Map Protocol Conformance Tab	17-33
DNS Map Filtering Tab	17-34
DNS Umbrella Connector Tab	17-35
DNS Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes	17-36
Configuring ESMTP Maps	17-39
ESMTP Policy Maps Add or Edit Match Condition and Action Dialog Boxes	17-40
Configuring FTP Maps	17-42
FTP Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes	17-43
Configuring GTP Maps	17-45
Add and Edit Country Network Codes Dialog Boxes	17-48
Add and Edit Permit Response Dialog Boxes	17-48
GTP Map Timeouts Dialog Box	17-48
GTP Policy Maps Add or Edit Match Condition and Action Dialog Boxes	17-49
Configuring H.323 Maps	17-51
Add or Edit HSI Group Dialog Boxes	17-53
Add or Edit HSI Endpoint IP Address Dialog Boxes	17-54
H.323 Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes	17-54
Configuring HTTP Maps for ASA 7.1.x, PIX 7.1.x, FWSM 3.x and IOS Devices	17-56
HTTP Map General Tab	17-57
HTTP Map Entity Length Tab	17-58
HTTP Map RFC Request Method Tab	17-60
HTTP Map Extension Request Method Tab	17-61
HTTP Map Port Misuse Tab	17-62
HTTP Map Transfer Encoding Tab	17-63
Configuring HTTP Maps for ASA 7.2+ and PIX 7.2+ Devices	17-64

- HTTP Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes **17-66**
- Configuring IM Maps for ASA 7.2+, PIX 7.2+ Devices **17-70**
 - IM Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes **17-71**
- Configuring IM Maps for IOS Devices **17-73**
- Configuring IP Options Maps **17-75**
- Configuring IPv6 Maps **17-77**
 - IPv6 Policy Maps Add or Edit Match Condition and Action Dialog Boxes **17-78**
- Configuring IPsec Pass Through Maps **17-80**
- Configuring NetBIOS Maps **17-81**
- Configuring ScanSafe Maps **17-82**
- Configuring SIP Maps **17-83**
 - SIP Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes **17-85**
- Configuring Skinny Maps **17-87**
 - Skinny Policy Maps Add or Edit Match Condition and Action Dialog Boxes **17-89**
- Configuring SNMP Maps **17-90**
- Configuring SCTP Maps **17-91**
 - SCTP Policy Maps Add or Edit Match Condition and Action Dialog Boxes **17-92**
- Configuring Diameter Maps **17-93**
 - Diameter Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes **17-95**
 - Create and Add Custom AVPs **17-97**
 - Create and Add TLS Proxy Objects **17-99**
- Configuring LISP Maps **17-102**
- Configuring M3UA Maps **17-103**
 - M3UA Protocol Conformance **17-103**
 - M3UA Inspection Limitations **17-103**
 - M3UA Policy Maps Add or Edit Match Condition and Action Dialog Boxes **17-105**
- Configuring Regular Expression Groups **17-108**
 - Add/Edit Regular Expressions **17-108**
 - Metacharacters Used to Build Regular Expressions **17-109**
- Configuring Settings for Inspection Rules for IOS Devices **17-111**

CHAPTER 18

Managing Firewall Web Filter Rules 18-1

- Understanding Web Filter Rules **18-1**
- Configuring Web Filter Rules for ASA, PIX, and FWSM Devices **18-2**
 - Web Filter Rules Page (ASA/PIX/FWSM) **18-3**
 - Add and Edit PIX/ASA/FWSM Web Filter Rule Dialog Boxes **18-5**
 - Edit Web Filter Type Dialog Box **18-8**
 - Edit Web Filter Options Dialog Box **18-9**

Configuring Web Filter Rules for IOS Devices	18-10
Web Filter Rules Page (IOS)	18-12
IOS Web Filter Rule and Applet Scanner Dialog Box	18-13
IOS Web Filter Exclusive Domain Name Dialog Box	18-14
Configuring Settings for Web Filter Servers	18-15
Web Filter Settings Page	18-16
Web Filter Server Configuration Dialog Box	18-19

CHAPTER 19**Managing Firewall Botnet Traffic Filter Rules 19-1**

Understanding Botnet Traffic Filtering	19-1
Task Flow for Configuring the Botnet Traffic Filter	19-2
Configuring the Dynamic Database	19-4
Adding Entries to the Static Database	19-5
Enabling DNS Snooping	19-6
Enabling Traffic Classification and Actions for the Botnet Traffic Filter	19-6
Botnet Traffic Filter Rules Page	19-9
Dynamic Blacklist Configuration Tab	19-10
Traffic Classification Tab	19-11
BTF Enable Rules Editor	19-12
BTF Drop Rules Editor	19-13
Whitelist/Blacklist Tab	19-14
Device Whitelist or Device Blacklist Dialog Box	19-15

CHAPTER 20**Working with ScanSafe Web Security 20-1**

Configuring ScanSafe Web Security	20-2
ScanSafe Web Security Page	20-4
Add and Edit Default User Groups Dialog Box	20-6
ScanSafe Web Security Settings Page	20-6

CHAPTER 21**Managing Zone-based Firewall Rules 21-1**

Understanding the Zone-based Firewall Rules	21-3
The Self Zone	21-5
Using VPNs with Zone-based Firewall Policies	21-6
Zones and VRF-aware Firewalls	21-7
Understanding the Relationship Between Permit/Deny and Action in Zone-based Firewall Rules	21-8
Understanding the Relationship Between Services and Protocols in Zone-based Firewall Rules	21-11
General Recommendations for Zone-based Firewall Rules	21-12
Developing and Applying Zone-based Firewall Rules	21-12

Adding Zone-Based Firewall Rules	21-13
Configuring Inspection Maps for Zone-based Firewall Policies	21-16
Configuring Class Maps for Zone-Based Firewall Policies	21-19
Zone-based Firewall IM Application Class Maps: Add or Edit Match Condition Dialog Boxes	21-21
Zone-based Firewall P2P Application Class Maps: Add or Edit Match Condition Dialog Boxes	21-21
H.323 (IOS) Class Maps Add or Edit Match Criterion Dialog Boxes	21-22
HTTP (IOS) Class Add or Edit Match Criterion Dialog Boxes	21-22
IMAP and POP3 Class Maps Add or Edit Match Criterion Dialog Boxes	21-25
SIP (IOS) Class Add or Edit Match Criterion Dialog Boxes	21-25
SMTP Class Maps Add or Edit Match Criterion Dialog Boxes	21-27
Sun RPC Class Maps Add or Edit Match Criterion Dialog Boxes	21-29
Local Web Filter Class Add or Edit Match Criterion Dialog Boxes	21-29
N2H2 and Websense Class Add or Edit Match Criterion Dialog Boxes	21-30
Configuring Inspect Parameter Maps	21-31
Configuring Protocol Info Parameter Maps	21-33
Add or Edit DNS Server for Protocol Info Parameters Dialog Box	21-34
Configuring Policy Maps for Zone-Based Firewall Policies	21-34
Add or Edit Match Condition and Action Dialog Boxes for Zone-Based Firewall and Web Filter Policies	21-35
Configuring Content Filtering Maps for Zone-based Firewall Policies	21-36
Configuring Local Web Filter Parameter Maps	21-38
Configuring N2H2 or WebSense Parameter Maps	21-39
Add or Edit External Filter Dialog Box	21-41
Configuring Trend Parameter Maps	21-42
Configuring URL Filter Parameter Maps	21-43
Add or Edit URL Domain Name Dialog Box for URL Filter Parameters	21-45
Configuring URLF Glob Parameter Maps	21-45
Configuring Web Filter Maps	21-47
Changing the Default Drop Behavior	21-48
Configuring Settings for Zone-based Firewall Rules	21-49
Zone Based Firewall Page	21-50
Zone Based Firewall Page - Content Filter Tab	21-52
Zone Dialog Box	21-53
Troubleshooting Zone-based Rules and Configurations	21-54
Zone-based Firewall Rules Page	21-58
Adding and Editing Zone-based Firewall Rules	21-62
Zone-based Firewall Rule: Advanced Options Dialog Box	21-67
Protocol Selector Dialog Box	21-68

Configure Protocol Dialog Box 21-69

CHAPTER 22

Managing Traffic Zones 22-1

- Why Use Zones? 22-1
- ECMP Routing 22-4
- Understanding Traffic Zones 22-6
- Prerequisites for Traffic Zones 22-7
- Guidelines for Traffic Zones 22-8
- Configuring Traffic Zones 22-9

CHAPTER 23

Managing Transparent Firewall Rules 23-1

- Configuring Transparent Firewall Rules 23-1
- Transparent Rules Page 23-3
 - Add and Edit Transparent Firewall Rule Dialog Boxes 23-5
 - Edit Transparent EtherType Dialog Box 23-7
 - Edit Transparent Mask Dialog Box 23-7

CHAPTER 24

Configuring Network Address Translation 24-1

- Understanding Network Address Translation 24-2
 - Types of Address Translation 24-3
 - About “Simplified” NAT on ASA 8.3+ Devices 24-4
- NAT Policies on Cisco IOS Routers 24-5
 - NAT Page: Interface Specification 24-6
 - NAT Page: Static Rules 24-6
 - NAT Static Rule Dialog Boxes 24-7
 - NAT Page: Dynamic Rules 24-10
 - NAT Dynamic Rule Dialog Box 24-11
 - NAT Page: Timeouts 24-13
- NAT Policies on Security Devices 24-15
 - NAT in Transparent Mode 24-16
 - Global Options Page 24-16
 - Translation Options Page 24-17
 - Configuring NAT on PIX, FWSM, and pre-8.3 ASA Devices 24-18
 - Address Pools 24-19
 - Translation Rules: PIX, FWSM, and pre-8.3 ASA 24-20
 - Translation Exemptions (NAT 0 ACL) 24-21
 - Dynamic Rules Tab 24-23
 - Policy Dynamic Rules Tab 24-25

Static Rules Tab	24-27
General Tab	24-32
Configuring NAT on ASA 8.3+ Devices	24-34
Translation Rules: ASA 8.3+	24-35
Per-Session NAT Rules: ASA 9.0(1)+	24-47

PART 3

VPN Configuration

CHAPTER 25

Managing Site-to-Site VPNs: The Basics 25-1

Understanding VPN Topologies	25-2
Hub-and-Spoke VPN Topologies	25-2
Point-to-Point VPN Topologies	25-3
Full Mesh VPN Topologies	25-4
Implicitly Supported Topologies	25-5
Understanding IPsec Technologies and Policies	25-5
Understanding Mandatory and Optional Policies for Site-to-Site VPNs	25-6
Overview of Site-to-Site VPN Policies	25-8
Understanding Devices Supported by Each IPsec Technology	25-9
Including Unmanaged or Non-Cisco Devices in a VPN	25-11
Understanding and Configuring VPN Default Policies	25-12
Using Device Overrides to Customize VPN Policies	25-13
Understanding VRF-Aware IPsec	25-14
VRF-Aware IPsec One-Box Solution	25-14
VRF-Aware IPsec Two-Box Solution	25-15
Enabling and Disabling VRF on Catalyst Switches and 7600 Devices	25-17
Accessing Site-to-Site VPN Topologies and Policies	25-17
Site-to-Site VPN Manager Window	25-18
Configuring VPN Topologies in Device View	25-19
Site-To-Site VPN Discovery	25-20
Supported and Unsupported Technologies and Topologies for VPN Discovery	25-20
Prerequisites for VPN Discovery	25-21
VPN Discovery Rules	25-22
Discovering Site-to-Site VPNs	25-24
Defining or Repairing Discovered VPNs with Multiple Spoke Definitions	25-26
Rediscovering Site-to-Site VPNs	25-27
Creating or Editing VPN Topologies	25-28
Defining the Name and IPsec Technology of a VPN Topology	25-30
Selecting Devices for Your VPN Topology	25-32
Defining the Endpoints and Protected Networks	25-34

Configuring VPN Interface Endpoint Settings	25-36
Configuring Dial Backup	25-40
Dial Backup Settings Dialog Box	25-41
Configuring VPNISM or VPN SPA/VSPA Endpoint Settings	25-42
Identifying the Protected Networks for Endpoints	25-46
Configuring a Firewall Services Module (FWSM) Interface with VPNISM or VPNSPA/VSPA	25-47
Configuring VRF Aware IPsec Settings	25-48
Configuring Crypto Map	25-50
Configuring High Availability in Your VPN Topology	25-52
Defining GET VPN Group Encryption	25-54
Add Certificate Filter Dialog Box	25-58
Add New or Edit Security Association Dialog Box	25-58
Defining GET VPN Peers	25-60
Assigning Initial Policies (Defaults) to a New VPN Topology	25-62
Viewing a Summary of a VPN Topology's Configuration	25-63
Creating or Editing Extranet VPNs	25-66
Deleting a VPN Topology	25-71

CHAPTER 26

Configuring IKE and IPsec Policies	26-1
Overview of IKE and IPsec Configurations	26-2
Comparing IKE Version 1 and 2	26-4
Understanding IKE	26-5
Deciding Which Encryption Algorithm to Use	26-6
Deciding Which Hash Algorithm to Use	26-6
Deciding Which Diffie-Hellman Modulus Group to Use	26-7
Deciding Which Authentication Method to Use	26-8
Configuring an IKE Proposal	26-9
Configuring IKEv1 Proposal Policy Objects	26-10
Configuring IKEv2 Proposal Policy Objects	26-14
Understanding IPsec Proposals	26-18
Understanding IPsec Proposals for Site-to-Site VPNs	26-19
Understanding Crypto Maps	26-19
Understanding Transform Sets	26-20
Understanding Reverse Route Injection	26-21
Configuring IPsec Proposals in Site-to-Site VPNs	26-22
Selecting the IKE Version for Devices in Site-to-Site VPNs	26-26
Configuring IPsec IKEv1 or IKEv2 Transform Set Policy Objects	26-27
Configuring VPN Global Settings	26-30

- Configuring VPN Global Address Assignment Settings 26-31
- Configuring VPN Global ISAKMP/IPsec Settings 26-33
- Configuring VPN Global IKEv2 Settings 26-37
- Understanding NAT in VPNs 26-41
- Configuring VPN Global NAT Settings 26-42
- Configuring VPN Global General Settings 26-44
- Understanding IKEv1 Preshared Key Policies in Site-to-Site VPNs 26-47
 - Configuring IKEv1 Preshared Key Policies 26-48
- Understanding Public Key Infrastructure Policies 26-51
 - Requirements for Successful PKI Enrollment 26-52
 - Configuring IKEv1 Public Key Infrastructure Policies in Site-to-Site VPNs 26-54
 - Defining Multiple IKEv1 CA Servers for Site-to-Site VPNs 26-55
 - Configuring Public Key Infrastructure Policies for Remote Access VPNs 26-56
 - PKI Enrollment Dialog Box 26-58
 - PKI Enrollment Dialog Box—CA Information Tab 26-60
 - PKI Enrollment Dialog Box—Enrollment Parameters Tab 26-63
 - PKI Enrollment Dialog Box—Certificate Subject Name Tab 26-66
 - PKI Enrollment Dialog Box—Trusted CA Hierarchy Tab 26-67
- Configuring IKEv2 Authentication in Site-to-Site VPNs 26-68
 - IKEv2 Authentication Policy 26-70
 - IKEv2 Authentication (Override) Dialog Box 26-72

CHAPTER 27

GRE and DM VPNs 27-1

- Understanding the GRE Modes Page 27-1
- GRE and Dynamic GRE VPNs 27-2
 - Understanding GRE 27-2
 - Advantages of IPsec Tunneling with GRE 27-3
 - How Does Security Manager Implement GRE? 27-3
 - Prerequisites for Successful Configuration of GRE 27-3
 - Understanding GRE Configuration for Dynamically Addressed Spokes 27-5
 - Configuring IPsec GRE VPNs 27-5
 - Configuring GRE Modes for GRE or GRE Dynamic IP VPNs 27-6
- Dynamic Multipoint VPNs (DMVPN) 27-9
 - Understanding DMVPN 27-10
 - Enabling Spoke-to-Spoke Connections in DMVPN Topologies 27-10
 - Advantages of DMVPN with GRE 27-11
 - Configuring DMVPN 27-12
 - Configuring GRE Modes for DMVPN 27-12
 - Configuring Large Scale DMVPNs 27-16

Configuring Server Load Balancing in Large Scale DMVPN	27-17
Edit Load Balancing Parameters Dialog Box	27-17

CHAPTER 28**Easy VPN 28-1**

Understanding Easy VPN	28-1
Easy VPN with Dial Backup	28-2
Easy VPN with High Availability	28-2
Easy VPN with Dynamic Virtual Tunnel Interfaces	28-3
Easy VPN Configuration Modes	28-3
Easy VPN and IKE Extended Authentication (Xauth)	28-4
Overview of Configuring Easy VPN	28-5
Important Notes About Easy VPN Configuration	28-6
Configuring Client Connection Characteristics for Easy VPN	28-7
Configuring Credentials Policy Objects	28-9
Configuring an IPsec Proposal for Easy VPN	28-10
Configuring Dynamic VTI for Easy VPN	28-12
Configuring a Connection Profile Policy for Easy VPN	28-13
Configuring a User Group Policy for Easy VPN	28-14

CHAPTER 29**Group Encrypted Transport (GET) VPNs 29-1**

Understanding Group Encrypted Transport (GET) VPNs	29-2
Understanding the GET VPN Registration Process	29-4
Choosing the Rekey Transport Mechanism	29-6
Configuring Redundancy Using Cooperative Key Servers	29-7
Configuring Fail-Close to Protect Registration Failures	29-8
Understanding the GET VPN Security Policy and Security Associations	29-10
Understanding Time-Based Anti-Replay	29-11
Configuring GET VPN	29-12
Generating and Synchronizing RSA Keys	29-13
Configuring the IKE Proposal for GET VPN	29-15
Configuring Global Settings for GET VPN	29-16
Configuring GET VPN Key Servers	29-18
Add Key Server, Group Member Dialog Box	29-19
Edit Key Server Dialog Box	29-19
Configuring GET VPN Group Members	29-20
Edit Group Member Dialog Box	29-21
Using Passive Mode to Migrate to GET VPN	29-23
Troubleshooting GET VPN Configurations	29-25

CHAPTER 30

Managing Remote Access VPNs: The Basics 30-1

- Understanding Remote Access VPNs 30-1
 - Understanding Remote Access IPsec VPNs 30-2
 - Understanding Remote Access SSL VPNs 30-2
 - Remote Access SSL VPN Example 30-3
 - SSL VPN Access Modes 30-4
 - Understanding and Managing SSL VPN Support Files 30-5
 - Prerequisites for Configuring SSL VPNs 30-7
 - SSL VPN Limitations 30-8
- Understanding Devices Supported by Each Remote Access VPN Technology 30-8
- Overview of Remote Access VPN Policies 30-9
- Discovering Remote Access VPN Policies 30-12
- Using the Remote Access VPN Configuration Wizard 30-13
 - Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (ASA Devices) 30-14
 - SSL VPN Configuration Wizard—Access Page (ASA) 30-16
 - SSL VPN Configuration Wizard—Connection Profile Page (ASA) 30-17
 - Creating User Groups with the Create Group Policy Wizard 30-20
 - Create Group Policy Wizard—Full Tunnel Page 30-21
 - Create Group Policy Wizard—Clientless and Thin Client Access Modes Page 30-24
 - Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard (ASA and PIX 7.0+ Devices) 30-25
 - Remote Access VPN Configuration Wizard—IPsec VPN Connection Profile Page (ASA) 30-28
 - Remote Access VPN Configuration Wizard—IPsec Settings Page (ASA) 30-30
 - Remote Access VPN Configuration Wizard—Defaults Page 30-31
 - Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (IOS Devices) 30-32
 - SSL VPN Configuration Wizard—Gateway and Context Page (IOS) 30-33
 - SSL VPN Configuration Wizard—Portal Page Customization Page (IOS) 30-35
 - Creating IPsec VPNs Using the Remote Access VPN Configuration Wizard (IOS and PIX 6.3 Devices) 30-36

CHAPTER 31

Managing Remote Access VPNs on ASA and PIX 7.0+ Devices 31-1

- Overview of Remote Access VPN Policies for ASA and PIX 7.0+ Devices 31-2
- Understanding Cluster Load Balancing (ASA) 31-5
 - Configuring Cluster Load Balance Policies (ASA) 31-5
- Configuring Connection Profiles (ASA, PIX 7.0+) 31-7
 - Connection Profiles Page 31-8
 - Supported CLIs in Remote Access VPN Multi-Context Mode - Connection Profiles 31-9
 - General Tab (Connection Profiles) 31-10
 - AAA Tab (Connection Profiles) 31-13

Secondary AAA Tab (Connection Profiles)	31-17
IPSec Tab (Connection Profiles)	31-19
SSL Tab (Connection Profiles)	31-22
Configuring Group Policies for Remote Access VPNs	31-26
Understanding Group Policies (ASA)	31-27
Creating Group Policies (ASA, PIX 7.0+)	31-28
Understanding SSL VPN Server Verification (ASA)	31-30
Configuring Trusted Pool Settings (ASA)	31-31
Using the Trustpool Manager	31-32
Add/Edit Scripts Dialog Box	31-34
Working with IPSec VPN Policies	31-36
Configuring Certificate to Connection Profile Map Policies (ASA)	31-36
Configuring Certificate to Connection Profile Map Rules (ASA)	31-37
Map Rule Dialog Box (Upper Table)	31-39
Map Rule Dialog Box (Lower Table)	31-40
Configuring an IPsec Proposal on a Remote Access VPN Server (ASA, PIX 7.0+ Devices)	31-40
IPsec Proposal Editor (ASA, PIX 7.0+ Devices)	31-41
Working with SSL and IKEv2 IPSec VPN Policies	31-44
Understanding SSL VPN Access Policies (ASA)	31-44
SSL VPN Access Policy Page	31-45
Configuring an Access Policy	31-50
Configuring Other SSL VPN Settings (ASA)	31-51
Configuring SSL VPN Performance Settings (ASA)	31-52
Configuring SSL VPN Content Rewrite Rules (ASA)	31-53
Configuring SSL VPN Encoding Rules (ASA)	31-55
Configuring SSL VPN Proxies and Proxy Bypass (ASA)	31-57
Configuring SSL VPN Browser Plug-ins (ASA)	31-60
Understanding SSL VPN AnyConnect Client Settings	31-62
Configuring SSL VPN AnyConnect Client Settings (ASA)	31-64
Understanding Kerberos Constrained Delegation (KCD) for SSL VPN (ASA)	31-67
Configuring Kerberos Constrained Delegation (KCD) for SSL VPN (ASA)	31-69
Configuring AnyConnect Custom Attributes (ASA)	31-70
Configuring SSL VPN Advanced Settings (ASA)	31-72
Configuring SSL VPN Server Verification (ASA)	31-73
Configuring SSL VPN Shared Licenses (ASA 8.2+)	31-74
Configuring an ASA Device as a Shared License Client	31-76
Configuring an ASA Device as a Shared License Server	31-77
Customizing Clientless SSL VPN Portals	31-77
Configuring ASA Portal Appearance Using SSL VPN Customization Objects	31-78

Localizing SSL VPN Web Pages for ASA Devices	31-80
Creating Your Own SSL VPN Logon Page for ASA Devices	31-82
Configuring SSL VPN Bookmark Lists for ASA and IOS Devices	31-82
Using the Post URL Method and Macro Substitutions in SSL VPN Bookmarks	31-84
Configuring SSL VPN Smart Tunnels for ASA Devices	31-85
Configuring WINS/NetBIOS Name Service (NBNS) Servers To Enable File System Access in SSL VPNs	31-88

CHAPTER 32

Managing Dynamic Access Policies for Remote Access VPNs (ASA 8.0+ Devices) 32-1

Understanding Dynamic Access Policies	32-1
Configuring Dynamic Access Policies	32-2
Understanding DAP Attributes	32-4
Configuring DAP Attributes	32-7
Configuring Cisco Secure Desktop Policies on ASA Devices	32-9
Dynamic Access Page (ASA)	32-11
Add/Edit Dynamic Access Policy Dialog Box	32-12
Main Tab	32-14
Logical Operations Tab	32-42
Advanced Expressions Tab	32-44
Cisco Secure Desktop Manager Policy Editor Dialog Box	32-46

CHAPTER 33

Managing Remote Access VPNs on IOS and PIX 6.3 Devices 33-1

Overview of Remote Access VPN Policies for IOS and PIX 6.3 Devices	33-2
Configuring an IPsec Proposal on a Remote Access VPN Server (IOS, PIX 6.3 Devices)	33-3
IPsec Proposal Editor (IOS, PIX 6.3 Devices)	33-4
VPNISM/VPN SPA/VSPA Settings Dialog Box	33-6
Configuring Dynamic VTI/VRF Aware IPsec in Remote Access VPNs (IOS Devices)	33-7
Configuring High Availability in Remote Access VPNs (IOS)	33-11
Configuring User Group Policies	33-13
Configuring an SSL VPN Policy (IOS)	33-14
SSL VPN Context Editor Dialog Box (IOS)	33-15
General Tab	33-16
Creating Cisco Secure Desktop Configuration Objects	33-18

CHAPTER 34

Configuring Policy Objects for Remote Access VPNs 34-1

ASA Group Policies Dialog Box	34-1
Override ASA Group Policy	34-4
Supported CLIs in Remote Access VPN Multi-Context Mode - Group Policy	34-5
ASA Group Policies Client Configuration Settings	34-6

ASA Group Policies Client Firewall Attributes	34-7
ASA Group Policies Hardware Client Attributes	34-9
ASA Group Policies IPsec Settings	34-10
Add or Edit Client Access Rules Dialog Box	34-12
ASA Group Policies SSL VPN Clientless Settings	34-12
Add or Edit VDI Server Dialog Box	34-15
ASA Group Policies SSL VPN Full Client Settings	34-19
ASA Group Policies SSL VPN Settings	34-25
Add or Edit Auto Signon Rules Dialog Box	34-27
ASA Group Policies Browser Proxy Settings	34-29
ASA Group Policies DNS/WINS Settings	34-30
ASA Group Policies Split Tunneling Settings	34-31
ASA Group Policies Connection Settings	34-33
Add or Edit Secure Desktop Configuration Dialog Box	34-35
Add and Edit File Object Dialog Boxes	34-37
File Object — Choose a file Dialog Box	34-39
Add or Edit Port Forwarding List Dialog Boxes	34-40
Add or Edit A Port Forwarding Entry Dialog Box	34-41
Add or Edit Single Sign On Server Dialog Boxes	34-42
Add or Edit Bookmarks Dialog Boxes	34-44
Add or Edit Bookmark Entry Dialog Boxes	34-45
Add and Edit Post Parameter Dialog Boxes	34-48
Add and Edit SSL VPN Customization Dialog Boxes	34-51
SSL VPN Customization Dialog Box—Title Panel	34-53
SSL VPN Customization Dialog Box—Language	34-54
Add and Edit Language Dialog Boxes	34-56
SSL VPN Customization Dialog Box—Logon Form	34-56
SSL VPN Customization Dialog Box—Informational Panel	34-57
SSL VPN Customization Dialog Box—Copyright Panel	34-58
SSL VPN Customization Dialog Box—Full Customization	34-59
SSL VPN Customization Dialog Box—Toolbar	34-59
SSL VPN Customization Dialog Box—Applications	34-60
SSL VPN Customization Dialog Box—Custom Panes	34-61
Add and Edit Column Dialog Boxes	34-61
Add or Edit Custom Pane Dialog Boxes	34-62
SSL VPN Customization Dialog Box—Home Page	34-62
SSL VPN Customization Dialog Box—Logout Page	34-63
Add or Edit SSL VPN Gateway Dialog Box	34-64
Add and Edit Smart Tunnel List Dialog Boxes	34-66

Add and Edit A Smart Tunnel Entry Dialog Boxes	34-67
Add and Edit Smart Tunnel Network Lists Dialog Boxes	34-69
Add and Edit A Smart Tunnel Network List Entry Dialog Box	34-70
Add and Edit Smart Tunnel Auto Signon List Dialog Boxes	34-71
Add and Edit Smart Tunnel Auto Signon Entry Dialog Boxes	34-72
Add or Edit User Group Dialog Box	34-73
User Group Dialog Box—General Settings	34-75
User Group Dialog Box—DNS/WINS Settings	34-77
User Group Dialog Box—Split Tunneling	34-77
User Group Dialog Box—IOS Client Settings	34-78
User Group Dialog Box—IOS Xauth Options	34-80
User Group Dialog Box—IOS Client VPN Software Update	34-81
Add/Edit Client Update Dialog Box	34-81
User Group Dialog Box—Advanced PIX Options	34-82
User Group Dialog Box—Clientless Settings	34-83
User Group Dialog Box—Thin Client Settings	34-84
User Group Dialog Box—SSL VPN Full Tunnel Settings	34-84
User Group Dialog Box—SSL VPN Split Tunneling	34-86
User Group Dialog Box—Browser Proxy Settings	34-87
User Group Dialog Box—SSL VPN Connection Settings	34-88
Add or Edit WINS Server List Dialog Box	34-89
Add or Edit WINS Server Dialog Box	34-90

CHAPTER 35

Using Map View 35-1

Understanding Maps and Map View	35-1
Understanding the Map View Main Page	35-2
Map Toolbar	35-4
Using the Navigation Window	35-4
Maps Context Menus	35-5
Managed Device Node Context Menu	35-5
Multiple Selected Nodes Context Menu	35-6
VPN Connection Context Menu	35-6
Layer 3 Link Context Menu	35-7
Map Object Context Menu	35-7
Map Background Context Menu	35-7
Access Permissions for Maps	35-8
Working With Maps	35-8
Creating New or Default Maps	35-9
Opening Maps	35-10

Saving Maps	35-10
Deleting Maps	35-10
Exporting Maps	35-11
Arranging Map Elements	35-11
Panning, Centering, and Zooming Maps	35-11
Selecting Map Elements	35-12
Searching for Map Nodes	35-12
Using Linked Maps	35-13
Setting the Map Background Properties	35-13
Displaying Your Network on the Map	35-14
Understanding Map Elements	35-14
Displaying Managed Devices on the Map	35-16
Showing Containment of Catalyst Switches, Firewalls, and Adaptive Security Appliances	35-16
Using Map Objects To Represent Network Topology	35-17
Add Map Object and Node Properties Dialog Boxes	35-18
Select Policy Object Dialog Box	35-18
Interface Properties Dialog Box	35-19
Creating and Managing Layer 3 Links on the Map	35-19
Select Interfaces and Link Properties Dialog Boxes	35-20
Add Link Dialog Box	35-20
Managing VPNs in Map View	35-20
Displaying Existing VPNs on the Map	35-21
Creating VPN Topologies in Map View	35-21
Editing VPN Policies or Peers From the Map	35-22
Managing Device Policies in Map View	35-22
Performing Basic Policy Management in Map View	35-22
Managing Firewall Policies in Map View	35-23
Managing Firewall Settings in Map View	35-23

PART 4**IPS Configuration****CHAPTER 36****Getting Started with IPS Configuration 36-1**

Understanding IPS Network Sensing	36-2
Capturing Network Traffic	36-2
Correctly Deploying the Sensor	36-4
Tuning the IPS	36-4
Overview of IPS Configuration	36-5
Identifying Allowed Hosts	36-7
Configuring SNMP	36-8

- General SNMP Configuration Options 36-10
- SNMPv3 Users Tab 36-11
 - Add SNMPv3 User Dialog Box 36-12
- SNMP Trap Configuration Tab 36-13
 - SNMP Trap Communication Dialog Box 36-14
- Managing User Accounts and Password Requirements 36-15
 - Understanding IPS User Roles 36-15
 - Understanding Managed and Unmanaged IPS Passwords 36-16
 - Understanding How IPS Passwords are Discovered and Deployed 36-17
 - Configuring IPS User Accounts 36-18
 - Add User and Edit User Credentials Dialog Boxes 36-19
 - Configuring User Password Requirements 36-20
 - Configuring AAA Access Control for IPS Devices 36-21
- Identifying an NTP Server 36-23
- Identifying DNS Servers 36-24
- Identifying an HTTP Proxy Server 36-24
- IPS SSHv2 Known Host Keys 36-25
 - Add or Edit Known Host RSA Key Dialog Box 36-25
- Configuring IPS SSHv1 Fallback Settings 36-26
- Configuring the External Product Interface 36-26
 - External Product Interface Dialog Box 36-27
 - Posture ACL Dialog Box 36-29
- Configuring IPS Logging Policies 36-30
- IPS Health Monitor 36-31
- Configuring IPS Security Settings 36-32

CHAPTER 37

- Managing IPS Device Interfaces 37-1**
 - Understanding Interfaces 37-1
 - Understanding Interface Modes 37-2
 - Promiscuous Mode 37-2
 - Inline Interface Mode 37-3
 - Inline VLAN Pair Mode 37-3
 - VLAN Group Mode 37-4
 - Deploying VLAN Groups 37-5
 - Configuring Interfaces 37-6
 - Understanding the IPS Interfaces Policy 37-6
 - Viewing a Summary of IPS Interface Configuration 37-8
 - Configuring Physical Interfaces 37-9

Modify Physical Interface Map Dialog Box	37-10
Configuring Bypass Mode	37-12
Configuring CDP Mode	37-12
Configuring Inline Interface Pairs	37-13
Configuring Inline VLAN Pairs	37-14
Configuring VLAN Groups	37-15

CHAPTER 38**Configuring Virtual Sensors 38-1**

Understanding the Virtual Sensor	38-1
Advantages and Restrictions of Virtualization	38-3
Inline TCP Session Tracking Mode	38-3
Understanding Normalizer Mode	38-4
Assigning Interfaces to Virtual Sensors	38-4
Identifying the Virtual Sensors for a Device	38-5
Defining A Virtual Sensor	38-5
Virtual Sensor Dialog Box	38-7
Editing Policies for a Virtual Sensor	38-9
Deleting A Virtual Sensor	38-10

CHAPTER 39**Defining IPS Signatures 39-1**

Understanding Signatures	39-1
Obtaining Detailed Information About a Signature	39-2
Understanding Signature Inheritance	39-3
IPS Signature Purge	39-3
Configuring Signatures	39-4
Signatures Page	39-4
Apply Signature Threat Profiles	39-9
Signature Shortcut Menu	39-10
Edit, Add, Replace Action Dialog Boxes	39-12
Edit Fidelity Dialog Box	39-13
Viewing Signature Update Levels	39-13
Enabling and Disabling Signatures	39-14
Editing Signatures	39-14
Edit Signature or Add Custom Signature Dialog Boxes	39-15
Adding Custom Signatures	39-19
Engine Options	39-20
Cloning Signatures	39-21
Regular Expressions in Custom Signatures	39-22
Editing Signature Parameters (Tuning Signatures)	39-23

Edit Signature Parameters Dialog Box	39-24
Editing the Component List for Meta Engine Signatures	39-29
Obsoletes Dialog Box	39-30
Configuring Signature Settings	39-30

CHAPTER 40

Configuring Event Action Rules 40-1

Understanding the IPS Event Action Process	40-1
Understanding IPS Event Actions	40-2
Configuring Event Action Filters	40-4
Tips for Managing Event Action Filter Rules	40-6
Event Action Filters Page	40-7
Filter Item Dialog Box	40-9
Configuring Event Action Overrides	40-13
Add or Edit Event Action Rule Dialog Box	40-14
Configuring Risk Rating Policy Objects	40-15
Add or Edit Risk Rating Dialog Box	40-16
Configuring IPS Event Action Network Information	40-17
Configuring Target Value Ratings	40-17
Target Value Rating Dialog Box	40-19
Understanding Passive OS Fingerprinting	40-19
Configuring OS Identification (Cisco IPS 6.x and Later Sensors Only)	40-21
OS Map Dialog Box	40-22
Configuring Settings for Event Actions	40-23

CHAPTER 41

Managing IPS Anomaly Detection 41-1

Understanding Anomaly Detection	41-1
Worm Viruses	41-2
Anomaly Detection Modes	41-2
Anomaly Detection Zones	41-3
Knowing When to Turn Off Anomaly Detection	41-4
Configuring Anomaly Detection Signatures	41-4
Configuring Anomaly Detection	41-6
Configuring Anomaly Detection Learning Accept Mode	41-8
Understanding Anomaly Detection Thresholds and Histograms	41-9
Configuring Anomaly Detection Thresholds and Histograms	41-11
Dest Port or Protocol Map Dialog Box	41-12
Histogram Dialog Box	41-13

CHAPTER 42**Configuring Global Correlation 42-1**

- Understanding Global Correlation 42-1
 - Understanding Reputation 42-2
 - Understanding Network Participation 42-3
 - Global Correlation Requirements and Limitations 42-4
- Configuring Global Correlation Inspection and Reputation 42-5
- Configuring Network Participation 42-7

CHAPTER 43**Configuring Attack Response Controller for Blocking and Rate Limiting 43-1**

- Understanding IPS Blocking 43-1
 - Strategies for Applying Blocks 43-3
 - Understanding Rate Limiting 43-4
 - Understanding Router and Switch Blocking Devices 43-4
 - Understanding the Master Blocking Sensor 43-6
- Configuring IPS Blocking and Rate Limiting 43-7
- Blocking Page 43-8
 - General Tab, IPS Blocking Policy 43-10
 - User Profile Dialog Box 43-12
 - Master Blocking Sensor Dialog Box 43-13
 - Router, Firewall, Cat6K Device Dialog Box 43-14
 - Router Block Interface Dialog Box 43-15
 - Cat6k Block VLAN Dialog Box 43-16
 - Never Block Host or Network Dialog Boxes 43-17

CHAPTER 44**Managing IPS Sensors 44-1**

- Managing IPS Licenses 44-1
 - Updating IPS License Files 44-1
 - Redeploying IPS License Files 44-2
 - Automating IPS License File Updates 44-3
- Managing IPS Updates 44-4
 - Configuring the IPS Update Server 44-4
 - Checking for IPS Updates and Downloading Them 44-5
 - Automating IPS Updates 44-6
 - Manually Applying IPS Updates 44-7
- Managing IPS Certificates 44-10
- Rebooting IPS Sensors 44-12

CHAPTER 45

Configuring IOS IPS Routers 45-1

- Understanding Cisco IOS IPS 45-1
 - Understanding IPS Subsystems and Support of IOS IPS Revisions 45-2
 - Cisco IOS IPS Signature Scanning with Lightweight Signatures 45-2
 - Router Configuration Files and Signature Event Action Processor (SEAP) 45-3
 - Cisco IOS IPS Limitations and Restrictions 45-3
- Overview of Cisco IOS IPS Configuration 45-4
 - Initial Preparation of a Cisco IOS IPS Router 45-5
 - Selecting a Signature Category for Cisco IOS IPS 45-6
 - Configuring General Settings for Cisco IOS IPS 45-7
 - Configuring IOS IPS Interface Rules 45-9
 - IPS Rule Dialog Box 45-10
 - Pair Dialog Box 45-11

PART 5

PIX/ASA/FWSM Device Configuration

CHAPTER 46

Managing Firewall Devices 46-1

- Firewall Device Types 46-1
- Default Firewall Configurations 46-2
- Configuring Firewall Device Interfaces 46-3
 - Understanding Device Interfaces 46-3
 - Interfaces in Routed and Transparent Modes 46-5
 - Interfaces in Single and Multiple Contexts 46-5
 - About Asymmetric Routing Groups 46-6
 - Understanding ASA 5505 Ports and Interfaces 46-6
 - Configuring Subinterfaces (PIX/ASA) 46-7
 - Configuring Redundant Interfaces 46-8
 - Configuring EtherChannels 46-9
 - Configuring VNI Interfaces 46-15
 - Configuring Tunnel Interface 46-22
 - Establishing Regular IPSec VPN Tunnel 46-24
 - Configuring IPSec Policy for Tunnel Interface 46-24
 - Managing Device Interfaces, Hardware Ports, and Bridge Groups 46-26
 - Add/Edit Interface Dialog Box (PIX 6.3) 46-28
 - Add/Edit Interface Dialog Box (PIX 7.0+/ASA/FWSM) 46-31
 - Add/Edit Interface Dialog Box: Cisco Firepower 9000 (General and Advanced tabs) 46-40
 - Configuring Hardware Ports on an ASA 5505 46-61
 - Add/Edit Bridge Group Dialog Box 46-62
 - Advanced Interface Settings (PIX/ASA/FWSM) 46-68

Enabling Traffic between Interfaces with the Same Security Level	46-70
Managing the PPPoE Users List	46-71
Managing VPDN Groups	46-72
VXLAN	46-73
Configuring VXLAN Policy	46-73

CHAPTER 47**Configuring Bridging Policies on Firewall Devices 47-1**

About Bridging on Firewall Devices	47-1
Bridging Support for FWSM 3.1	47-3
ARP Table Page	47-3
Add/Edit ARP Configuration Dialog Box	47-5
ARP Inspection Page	47-5
Add/Edit ARP Inspection Dialog Box	47-6
Managing the IPv6 Neighbor Cache	47-7
MAC Address Table Page	47-8
Add/Edit MAC Table Entry Dialog Box	47-8
MAC Learning Page	47-9
Add/Edit MAC Learning Dialog Box	47-9
Management IP Page	47-10
Management IPv6 Page (ASA 5505)	47-11

CHAPTER 48**Configuring Device Administration Policies on Firewall Devices 48-1**

About AAA on Security Devices	48-1
Preparing for AAA	48-2
Local Database	48-3
AAA for Device Administration	48-4
AAA for Network Access	48-4
AAA for VPN Access	48-4
Configuring AAA - Authentication Tab	48-5
Authorization Tab	48-7
Accounting Tab	48-8
Configuring Banners	48-9
Configuring Boot Image/Configuration Settings	48-10
Images Dialog Box	48-12
Configuring CLI Prompt	48-12
Setting the Device Clock	48-14
Enabling/Disabling FIPS	48-15

- Configuring Umbrella Global Policy 48-16
- Configuring Device Credentials 48-17
- Managing Mount Points 48-19
 - Add/Edit Mount Point Configuration Dialog Box 48-19
- IP Client 48-20
 - Add/Edit IP Client Dialog Box 48-21
- App Agent 48-21

CHAPTER 49

Configuring Device Access Settings on Firewall Devices 49-1

- Configuring Console Timeout 49-1
- HTTP Page 49-2
 - HTTP Configuration Dialog Box 49-3
- Configuring ICMP 49-4
 - Add and Edit ICMP Dialog Boxes 49-5
- Configuring Management Access 49-6
- Configuring Management Session Quota Limits 49-7
- Configuring Secure Shell Access 49-7
 - Add and Edit SSH Host Dialog Boxes 49-8
- Configuring SSL - Basic and Advanced tabs 49-9
- Reference Identities 49-13
 - Add/Edit Reference Identity Dialog Box 49-13
- Configuring SNMP 49-14
 - SNMP Terminology 49-15
 - SNMP Version 3 49-15
 - SNMP Page 49-17
 - SNMP Trap Configuration Dialog Box 49-19
 - Add/Edit SNMP Host Access Entry Dialog Box 49-22
 - Add/Edit SNMP Host Group Entry Dialog Box 49-23
 - Add/Edit SNMP Group Entry Dialog Box 49-24
 - Add/Edit SNMP User Entry Dialog Box 49-25
 - Add/Edit SNMP User List Entry Dialog Box 49-27
- Telnet Page 49-29
 - Telnet Configuration Dialog Box 49-29

CHAPTER 50

Configuring Failover 50-1

- Understanding Failover 50-1
 - Active/Active Failover 50-3
 - Stateful Failover 50-4

Basic Failover Configuration	50-5
Adding A Security Context to Failover Group 2	50-8
Additional Steps for an Active/Standby Failover Configuration	50-9
Exporting the Certificate to a File or PKCS12 data	50-9
Importing the Certificate onto the Standby Device	50-9
Failover Policies	50-10
Failover Page (PIX 6.3)	50-10
Edit Failover Interface Configuration Dialog Box (PIX 6.3)	50-12
Failover Page (FWSM)	50-13
Advanced Settings Dialog Box	50-16
Failover Page (ASA/PIX 7.0+)	50-17
Settings Dialog Box	50-21
Failover Page (Security Context)	50-26
Bootstrap Configuration for LAN Failover Dialog Box	50-26

CHAPTER 51**Configuring Hostname, Resources, User Accounts, and SLAs** 51-1

Hostname Page	51-1
Resource Management on Multi-context FWSMs	51-2
Resources Page	51-3
Add and Edit Resource Dialog Boxes	51-4
Configuring User Accounts	51-7
Add/Edit User Account Dialog Boxes	51-7
Monitoring Service Level Agreements (SLAs) To Maintain Connectivity	51-8
Creating Service Level Agreements	51-9
Configuring SLA Monitor Objects	51-10

CHAPTER 52**Configuring Server Access Settings on Firewall Devices** 52-1

AUS Page	52-1
Add and Edit Auto Update Server Dialog Boxes	52-3
DHCP Relay Page	52-5
Add and Edit DHCP Relay Agent Configuration Dialog Boxes	52-6
Add and Edit DHCP Relay Server Configuration Dialog Boxes	52-7
DHCP Relay IPv6 Page	52-7
Add and Edit DHCP Relay IPv6 Agent Configuration Dialog Boxes	52-9
Add and Edit DHCP Relay IPv6 Server Configuration Dialog Boxes	52-9
Configuring DHCP Servers	52-10
DHCP Server Page	52-10
Add and Edit DHCP Server Interface Configuration Dialog Boxes	52-12

Add/Edit DHCP Server Advanced Configuration Dialog Box	52-13
DNS Page	52-14
Add DNS Server Group Dialog Box	52-16
Add DNS Server Dialog Box	52-17
Configuring DDNS	52-18
Add/Edit DDNS Interface Rule Dialog Box	52-19
DDNS Update Methods Dialog Box	52-19
NTP Page	52-21
NTP Server Configuration Dialog Box	52-21
SMTP Server Page	52-22
TFTP Server Page	52-23

CHAPTER 53

Configuring FXOS Server Access Settings on Firepower 2100 Series Devices 53-1

HTTPS Page	53-1
Add and Edit HTTPS Dialog Boxes	53-2
SSH Page	53-2
Add and Edit SSH Dialog Boxes	53-3
SNMP Page	53-4
Add and Edit SNMP Dialog Boxes	53-4

CHAPTER 54

Configuring Logging Policies on Firewall Devices 54-1

NetFlow Page	54-1
Add and Edit Collector Dialog Boxes (NetFlow)	54-2
Embedded Event Manager	54-3
Add and Edit Applet Dialog Boxes	54-5
Add and Edit Syslog Configuration Dialog Boxes	54-7
Add and Edit Action Configuration Dialog Boxes	54-7
E-Mail Setup Page	54-8
Add/Edit Email Recipient Dialog Box	54-8
Event Lists Page	54-9
Message Classes and Associated Message ID Numbers	54-9
Add/Edit Event List Dialog Box	54-10
Add/Edit Syslog Class Dialog Box	54-11
Add/Edit Syslog Message ID Filter Dialog Box	54-11
Logging Filters Page	54-12
Edit Logging Filters Dialog Box	54-13
Configuring Logging Setup	54-14
Logging Setup Page	54-15

Configuring Rate Limit Levels	54-17
Rate Limit Page	54-18
Add/Edit Rate Limit for Syslog Logging Levels Dialog Box	54-18
Add/Edit Rate Limited Syslog Message Dialog Box	54-19
Configuring Syslog Server Setup	54-20
Syslog Relay Configuration	54-21
Server Setup Page	54-21
Logging Levels	54-24
Add/Edit Syslog Message Dialog Box	54-25
Defining Syslog Servers	54-26
Syslog Servers Page	54-27
Add/Edit Syslog Server Dialog Box	54-28

CHAPTER 55**Configuring Multicast Policies on Firewall Devices 55-1**

Enabling PIM and IGMP	55-1
Configuring IGMP	55-2
IGMP Page - Protocol Tab	55-3
Configure IGMP Parameters Dialog Box	55-4
IGMP Page - Access Group Tab	55-5
Configure IGMP Access Group Parameters Dialog Box	55-5
IGMP Page - Static Group Tab	55-6
Configure IGMP Static Group Parameters Dialog Box	55-6
IGMP Page - Join Group Tab	55-7
Configure IGMP Join Group Parameters Dialog Box	55-7
Configuring Multicast Routes	55-8
Add/Edit MRoute Configuration Dialog Box	55-8
Configuring Multicast Boundary Filters	55-9
Add/Edit MBoundary Configuration Dialog Box	55-9
Add/Edit MBoundary Interface Configuration Dialog Box	55-10
Configuring PIM	55-11
PIM Page - Protocol Tab	55-11
Add/Edit PIM Protocol Dialog Box	55-12
PIM Page - Neighbor Filter Tab	55-12
Add/Edit PIM Neighbor Filter Dialog Box	55-13
PIM Page - Bidirectional Neighbor Filter Tab	55-13
Add/Edit PIM Bidirectional Neighbor Filter Dialog Box	55-14
PIM Page - Rendezvous Points Tab	55-15
Add/Edit Rendezvous Point Dialog Box	55-16
PIM Page - Route Tree Tab	55-17

PIM Page - Request Filter Tab 55-18
 Add/Edit Multicast Group Rules Dialog Box 55-19
 PIM Page - Bootstrap Router Tab 55-20
 Add/Edit Bootstrap Router Dialog Box 55-21

CHAPTER 56

Configuring Routing Policies on Firewall Devices 56-1

Configuring No Proxy ARP 56-1
 Configuring BGP 56-2
 About BGP 56-3
 General Tab 56-5
 IPv4 Family Tab 56-6
 IPv4 Family - General Tab 56-7
 Add/Edit Aggregate Address Dialog Box 56-9
 Add/Edit Filter Dialog Box 56-10
 Add/Edit Neighbor Dialog Box 56-11
 Add/Edit Network Dialog Box 56-17
 Add/Edit Redistribution Dialog Box 56-18
 Add/Edit Route Injection Dialog Box 56-19
 IPv6 Family Tab 56-20
 IPv6 Family - General Tab 56-21
 Add/Edit Aggregate Address Dialog Box 56-22
 Add/Edit Neighbor Dialog Box 56-24
 Add/Edit Network Dialog Box 56-29
 Add/Edit Redistribution Dialog Box 56-30
 Add/Edit Route Injection Dialog Box 56-31
 Configuring EIGRP 56-32
 About EIGRP 56-33
 EIGRP Advanced Dialog Box 56-34
 Setup Tab 56-36
 Filter Rules Tab 56-39
 Add/Edit EIGRP Filter Rule Dialog Box 56-40
 Neighbors Tab 56-41
 Add/Edit EIGRP Neighbor Dialog Box 56-42
 Redistribution Tab 56-42
 Add/Edit EIGRP Redistribution Dialog Box 56-44
 Summary Address Tab 56-45
 Add/Edit EIGRP Summary Address Dialog Box 56-46
 Interfaces Tab 56-47
 Add/Edit EIGRP Interface Dialog Box 56-48

Configuring ISIS	56-49
About ISIS	56-49
General Tab	56-49
IPv4 Family Tab	56-51
IPv4 Family Tab—General Tab	56-51
IPv4 Family Tab—SPF Tab	56-52
IPv4 Family Tab—Redistribution Tab	56-53
IPv6 Family Tab	56-55
IPv6 Family Tab—General Tab	56-55
IPv6 Family Tab—SPF Tab	56-55
IPv6 Family Tab—Redistribution Tab	56-57
IPv6 Family Tab—Summary Prefix	56-57
Authentication Tab	56-58
Link State Packet Tab	56-59
Summary Address Tab	56-60
Network Entity Title Tab	56-61
Interface Tab	56-61
Interface Tab—General Tab	56-62
Interface Tab—Authentication Tab	56-63
Interface Tab—Hello Padding Tab	56-64
Interface Tab—LSP Settings Tab	56-65
Interface Tab—Metrics Tab	56-65
Passive Interfaces Tab	56-66
Configuring BFD Routing	56-66
About BFD	56-66
BFD Asynchronous Mode and Echo Function	56-67
BFD Session Establishment	56-67
BFD Timer Negotiation	56-69
BFD Failure Detection	56-69
BFD Deployment Scenarios	56-70
Create BFD Template	56-70
Add/ Edit BFD Map Dialog Box	56-72
Add/ Edit BFD Interface Dialog Box	56-73
Configuring OSPF	56-75
About OSPF	56-75
General Tab	56-76
OSPF Advanced Dialog Box	56-77
Area Tab	56-81
Add/Edit Area/Area Networks Dialog Box	56-82
Range Tab	56-84

Add/Edit Area Range Network Dialog Box	56-84
Neighbors Tab	56-85
Add/Edit Static Neighbor Dialog Box	56-85
Redistribution Tab	56-86
Redistribution Dialog Box	56-87
Virtual Link Tab	56-89
Add/Edit OSPF Virtual Link Configuration Dialog Box	56-90
Add/Edit OSPF Virtual Link MD5 Configuration Dialog Box	56-91
Filtering Tab	56-92
Add/Edit Filtering Dialog Box	56-93
Filter Rule Tab	56-94
Add/Edit Filter Rule Dialog Box	56-95
Summary Address Tab	56-95
Add/Edit Summary Address Dialog Box	56-96
Interface Tab	56-97
Add/Edit Interface Dialog Box	56-98
Configuring Key Chain	56-101
Lifetime of a Key	56-101
Add/Edit Key Chain	56-102
Configuring OSPFv3	56-103
About OSPFv3	56-104
Process Tab	56-106
OSPFv3 Advanced Properties Dialog Box	56-107
Area Tab (OSPFv3)	56-111
Add/Edit Redistribution Dialog Box (OSPFv3)	56-115
Add/Edit Summary Prefix Dialog Box (OSPFv3)	56-116
OSPFv3 Interface Tab	56-117
Add/Edit Interface Dialog Box (OSPFv3)	56-117
Add/Edit Neighbor Dialog Box (OSPFv3)	56-121
Configuring RIP	56-122
RIP Page for PIX/ASA 6.3–7.1 and FWSM	56-123
Add/Edit RIP Configuration (PIX/ASA 6.3–7.1 and FWSM) Dialog Boxes	56-124
RIP Page for PIX/ASA 7.2 and Later	56-125
RIP - Setup Tab	56-126
RIP - Redistribution Tab	56-128
RIP - Filtering Tab	56-129
RIP - Interface Tab	56-130
Configuring Static Routes	56-131
Add/Edit Static Route Dialog Box	56-133

Add/Edit IPv6 Static Route Dialog Box	56-134
Configuring Policy Objects for ASA Routing Policies	56-135
Understanding Route Map Objects	56-135
Add or Edit Route Map Object Dialog Boxes	56-139
Add or Edit Policy List Object Dialog Box	56-146
Add or Edit Prefix List Object Dialog Box	56-149
Add or Edit Prefix List Entry Dialog Box	56-151
Add or Edit Prefix List IPv6 Object Dialog Box	56-151
Add or Edit IPv6 Prefix List Entry Dialog Box	56-153
Add or Edit As Path Object Dialog Boxes	56-154
Add or Edit As Path Entry Dialog Box	56-155
Add or Edit Community List Object Dialog Box	56-156
Add or Edit Community List Entry Dialog Box	56-157
Add or Edit Community List Entry Dialog Box	56-158

CHAPTER 57**Configuring Security Policies on Firewall Devices 57-1**

General Page	57-1
Configuring Floodguard, Anti-Spoofing and Fragment Settings	57-2
Add/Edit General Security Configuration Dialog Box	57-3
Configuring Timeouts	57-4

CHAPTER 58**Configuring Service Policy Rules on Firewall Devices 58-1**

About Service Policy Rules	58-1
About TCP State Bypass	58-3
Priority Queues Page	58-4
Priority Queue Configuration Dialog Box	58-4
Service Policy Rules Page	58-5
Insert/Edit Service Policy (MPC) Rule Wizard	58-6
Step 1. Configure a Service Policy	58-6
Step 2. Configure the traffic class	58-7
Step 3. Configure the MPC actions	58-8
About IPS Modules on ASA Devices	58-15
About the ASA CX	58-17
ASA CX Auth Proxy Configuration	58-17
Configuring Traffic Flow Objects	58-18
Default Inspection Traffic	58-20
Configuring TCP Maps	58-22
Add and Edit TCP Option Range Dialog Boxes	58-25

CHAPTER 59

Configuring Security Contexts on Firewall Devices 59-1

- Enabling and Disabling Multiple-Context Mode 59-1
- Checklist for Configuring Multiple Security Contexts 59-3
- Managing Security Contexts 59-7
 - Add/Edit Security Context Dialog Box (FWSM) 59-8
 - Add/Edit Security Context Dialog Box (PIX/ASA) 59-9
 - Allocate Interfaces Dialog Box (PIX/ASA only) 59-12

CHAPTER 60

User Preferences 60-1

- Configuring Deployment Preferences on Firewall Devices 60-1
- Configuring Transactional Commit Preferences on Firewall Devices 60-2

PART 6

Router and Switch Device Configuration

CHAPTER 61

Managing Routers 61-1

- Configuring Routers Running IOS Software Releases 12.1 and 12.2 61-3
- Discovering Router Policies 61-3

CHAPTER 62

Configuring Router Interfaces 62-1

- Basic Interface Settings on Cisco IOS Routers 62-1
 - Available Interface Types 62-2
 - Defining Basic Router Interface Settings 62-4
 - Deleting a Cisco IOS Router Interface 62-6
- Router Interfaces Page 62-7
 - Create Router Interface Dialog Box 62-8
 - Interface Auto Name Generator Dialog Box 62-12
- Advanced Interface Settings on Cisco IOS Routers 62-13
 - Understanding Helper Addresses 62-14
- Advanced Interface Settings Page 62-16
 - Advanced Interface Settings Dialog Box 62-16
- IPS Module Interface Settings on Cisco IOS Routers 62-22
 - IPS Module Interface Settings Page 62-23
 - IPS Monitoring Information Dialog Box 62-24
- CEF Interface Settings on Cisco IOS Routers 62-25
 - CEF Interface Settings Page 62-26
 - CEF Interface Settings Dialog Box 62-27
- Dialer Interfaces on Cisco IOS Routers 62-28

Defining Dialer Profiles	62-28
Defining BRI Interface Properties	62-30
Dialer Policy Page	62-31
Dialer Profile Dialog Box	62-32
Dialer Physical Interface Dialog Box	62-33
ADSL on Cisco IOS Routers	62-34
Supported ADSL Operating Modes	62-35
Defining ADSL Settings	62-36
ADSL Policy Page	62-37
ADSL Settings Dialog Box	62-38
SHDSL on Cisco IOS Routers	62-41
Defining SHDSL Controllers	62-41
SHDSL Policy Page	62-42
SHDSL Controller Dialog Box	62-43
Controller Auto Name Generator Dialog Box	62-46
PVCs on Cisco IOS Routers	62-47
Understanding Virtual Paths and Virtual Channels	62-47
Understanding ATM Service Classes	62-48
Understanding ATM Management Protocols	62-49
Understanding ILMI	62-50
Understanding OAM	62-51
Defining ATM PVCs	62-51
Defining OAM Management on ATM PVCs	62-54
PVC Policy Page	62-55
PVC Dialog Box	62-56
PVC Dialog Box—Settings Tab	62-58
PVC Dialog Box—QoS Tab	62-61
PVC Dialog Box—Protocol Tab	62-64
Define Mapping Dialog Box	62-65
PVC Advanced Settings Dialog Box	62-66
PVC Advanced Settings Dialog Box—OAM Tab	62-67
PVC Advanced Settings Dialog Box—OAM-PVC Tab	62-69
PPP on Cisco IOS Routers	62-71
Understanding Multilink PPP (MLP)	62-71
Defining PPP Connections	62-72
Defining Multilink PPP Bundles	62-75
PPP/MLP Policy Page	62-76
PPP Dialog Box	62-77
PPP Dialog Box—PPP Tab	62-78

PPP Dialog Box—MLP Tab 62-80

CHAPTER 63

Router Device Administration 63-1

- AAA on Cisco IOS Routers 63-2
 - Supported Authorization Types 63-2
 - Supported Accounting Types 63-3
 - Understanding Method Lists 63-3
 - Defining AAA Services 63-4
- AAA Policy Page 63-6
 - AAA Page—Authentication Tab 63-6
 - AAA Page—Authorization Tab 63-8
 - Command Authorization Dialog Box 63-10
 - AAA Page—Accounting Tab 63-10
 - Command Accounting Dialog Box 63-13
- User Accounts and Device Credentials on Cisco IOS Routers 63-14
 - Defining Accounts and Credential Policies 63-14
- Accounts and Credentials Policy Page 63-16
 - User Account Dialog Box 63-17
- Bridging on Cisco IOS Routers 63-18
 - Bridge-Group Virtual Interfaces 63-19
 - Defining Bridge Groups 63-20
- Bridging Policy Page 63-21
 - Bridge Group Dialog Box 63-21
- Time Zone Settings on Cisco IOS Routers 63-22
 - Defining Time Zone and DST Settings 63-22
- Clock Policy Page 63-23
- CPU Utilization Settings on Cisco IOS Routers 63-25
 - Defining CPU Utilization Settings 63-25
- CPU Policy Page 63-26
- HTTP and HTTPS on Cisco IOS Routers 63-28
 - Defining HTTP Policies 63-29
- HTTP Policy Page 63-31
 - HTTP Page—Setup Tab 63-31
 - HTTP Page—AAA Tab 63-32
 - Command Authorization Override Dialog Box 63-34
- Line Access on Cisco IOS Routers 63-35
 - Defining Console Port Setup Parameters 63-35
 - Defining Console Port AAA Settings 63-37

Defining VTY Line Setup Parameters	63-38
Defining VTY Line AAA Settings	63-40
Console Policy Page	63-42
Console Page—Setup Tab	63-42
Console Page—Authentication Tab	63-44
Console Page—Authorization Tab	63-45
Console Page—Accounting Tab	63-47
VTY Policy Page	63-50
VTY Line Dialog Box	63-51
VTY Line Dialog Box—Setup Tab	63-52
VTY Line Dialog Box—Authentication Tab	63-55
VTY Line Dialog Box—Authorization Tab	63-56
VTY Line Dialog Box—Accounting Tab	63-57
Command Authorization Dialog Box—Line Access	63-60
Command Accounting Dialog Box—Line Access	63-61
Optional SSH Settings on Cisco IOS Routers	63-63
Defining Optional SSH Settings	63-63
Secure Shell Policy Page	63-64
SNMP on Cisco IOS Routers	63-66
Defining SNMP Agent Properties	63-67
Enabling SNMP Traps	63-68
SNMP Policy Page	63-69
Permission Dialog Box	63-70
Trap Receiver Dialog Box	63-71
SNMP Traps Dialog Box	63-72
DNS on Cisco IOS Routers	63-74
Defining DNS Policies	63-75
DNS Policy Page	63-76
IP Host Dialog Box	63-76
Hostnames and Domain Names on Cisco IOS Routers	63-77
Defining Hostname Policies	63-77
Hostname Policy Page	63-78
Memory Settings on Cisco IOS Routers	63-78
Defining Router Memory Settings	63-78
Memory Policy Page	63-79
Secure Device Provisioning on Cisco IOS Routers	63-81
Contents of Bootstrap Configuration	63-82
Secure Device Provisioning Workflow	63-82

- Defining Secure Device Provisioning Policies 63-83
- Configuring a AAA Server Group for Administrative Introducers 63-84
- Secure Device Provisioning Policy Page 63-85
- DHCP on Cisco IOS Routers 63-87
 - Understanding DHCP Database Agents 63-88
 - Understanding DHCP Relay Agents 63-88
 - Understanding DHCP Option 82 63-89
 - Understanding Secured ARP 63-89
 - Defining DHCP Policies 63-90
 - Defining DHCP Address Pools 63-91
- DHCP Policy Page 63-92
 - DHCP Database Dialog Box 63-94
 - IP Pool Dialog Box 63-94
- NTP on Cisco IOS Routers 63-96
 - Defining NTP Servers 63-97
- NTP Policy Page 63-98
 - NTP Server Dialog Box 63-99

CHAPTER 64

- Configuring Identity Policies 64-1**
 - 802.1x on Cisco IOS Routers 64-1
 - Understanding 802.1x Device Roles 64-2
 - 802.1x Interface Authorization States 64-2
 - Topologies Supported by 802.1x 64-3
 - Defining 802.1x Policies 64-4
 - 802.1x Policy Page 64-5
 - Network Admission Control on Cisco IOS Routers 64-8
 - Router Platforms Supporting NAC 64-8
 - Understanding NAC Components 64-9
 - Understanding NAC System Flow 64-9
 - Defining NAC Setup Parameters 64-10
 - Defining NAC Interface Parameters 64-11
 - Defining NAC Identity Parameters 64-13
 - Network Admission Control Policy Page 64-14
 - Network Admission Control Page—Setup Tab 64-14
 - Network Admission Control Page—Interfaces Tab 64-16
 - NAC Interface Configuration Dialog Box 64-17
 - Network Admission Control Page—Identities Tab 64-18
 - NAC Identity Profile Dialog Box 64-19
 - NAC Identity Action Dialog Box 64-19

CHAPTER 65

Configuring Logging Policies	65-1
Logging on Cisco IOS Routers	65-1
Defining Syslog Logging Setup Parameters	65-1
Defining Syslog Servers	65-3
Understanding Log Message Severity Levels	65-4
NetFlow on Cisco IOS Routers	65-5
Defining NetFlow Parameters	65-6
Syslog Logging Setup Policy Page	65-7
Syslog Servers Policy Page	65-10
Syslog Server Dialog Box	65-11
NetFlow Policy Page	65-12
Adding and Editing NetFlow Interface Settings	65-15

CHAPTER 66

Configuring Quality of Service	66-1
Quality of Service on Cisco IOS Routers	66-1
Quality of Service and CEF	66-2
Understanding Matching Parameters	66-2
Understanding Marking Parameters	66-3
Understanding Queuing Parameters	66-4
Tail Drop vs. WRED	66-4
Low-Latency Queuing	66-5
Default Class Queuing	66-6
Understanding Policing and Shaping Parameters	66-6
Understanding the Token-Bucket Mechanism	66-8
Understanding Control Plane Policing	66-9
Defining QoS Policies	66-10
Defining QoS on Interfaces	66-10
Defining QoS on the Control Plane	66-12
Defining QoS Class Matching Parameters	66-13
Defining QoS Class Marking Parameters	66-15
Defining QoS Class Queuing Parameters	66-16
Defining QoS Class Policing Parameters	66-17
Defining QoS Class Shaping Parameters	66-18
Quality of Service Policy Page	66-19
QoS Policy Dialog Box	66-21
QoS Class Dialog Box	66-23
QoS Class Dialog Box—Matching Tab	66-24
Edit ACLs Dialog Box—QoS Classes	66-25
QoS Class Dialog Box—Marking Tab	66-26

QoS Class Dialog Box—Queuing and Congestion Avoidance Tab 66-27
 QoS Class Dialog Box—Policing Tab 66-29
 QoS Class Dialog Box—Shaping Tab 66-31

CHAPTER 67

Configuring Routing Policies 67-1

BGP Routing on Cisco IOS Routers 67-1
 Defining BGP Routes 67-2
 Redistributing Routes into BGP 67-3
 BGP Routing Policy Page 67-4
 BGP Page—Setup Tab 67-5
 Neighbors Dialog Box 67-6
 BGP Page—Redistribution Tab 67-7
 BGP Redistribution Mapping Dialog Box 67-7
 EIGRP Routing on Cisco IOS Routers 67-8
 Defining EIGRP Routes 67-9
 Defining EIGRP Interface Properties 67-10
 Redistributing Routes into EIGRP 67-12
 EIGRP Routing Policy Page 67-13
 EIGRP Page—Setup Tab 67-13
 EIGRP Setup Dialog Box 67-14
 EIGRP Page—Interfaces Tab 67-15
 EIGRP Interface Dialog Box 67-16
 EIGRP Page—Redistribution Tab 67-17
 EIGRP Redistribution Mapping Dialog Box 67-18
 OSPF Routing on Cisco IOS Routers 67-19
 Defining OSPF Process Settings 67-20
 Defining OSPF Area Settings 67-21
 Redistributing Routes into OSPF 67-22
 Defining OSPF Redistribution Mappings 67-22
 Defining OSPF Maximum Prefix Values 67-24
 Defining OSPF Interface Settings 67-25
 Understanding Interface Cost 67-26
 Understanding Interface Priority 67-26
 Disabling MTU Mismatch Detection 67-27
 Blocking LSA Flooding 67-28
 Understanding OSPF Timer Settings 67-28
 Understanding the OSPF Network Type 67-29
 Understanding OSPF Interface Authentication 67-29
 OSPF Interface Policy Page 67-30

OSPF Interface Dialog Box	67-31
OSPF Process Policy Page	67-34
OSPF Process Page—Setup Tab	67-35
OSPF Setup Dialog Box	67-35
Edit Interfaces Dialog Box—OSPF Passive Interfaces	67-36
OSPF Process Page—Area Tab	67-36
OSPF Area Dialog Box	67-37
OSPF Process Page—Redistribution Tab	67-38
OSPF Redistribution Mapping Dialog Box	67-39
OSPF Max Prefix Mapping Dialog Box	67-41
RIP Routing on Cisco IOS Routers	67-42
Defining RIP Setup Parameters	67-42
Defining RIP Interface Authentication Settings	67-43
Redistributing Routes into RIP	67-44
RIP Routing Policy Page	67-45
RIP Page—Setup Tab	67-45
RIP Page—Authentication Tab	67-46
RIP Authentication Dialog Box	67-47
RIP Page—Redistribution Tab	67-48
RIP Redistribution Mapping Dialog Box	67-49
Static Routing on Cisco IOS Routers	67-50
Defining Static Routes	67-50
Static Routing Policy Page	67-51
Static Routing Dialog Box	67-52
CHAPTER 68	Managing Cisco Catalyst Switches and Cisco 7600 Series Routers
	68-1
Discovering Policies on Cisco Catalyst Switches and Cisco 7600 Series Routers	68-1
Viewing Catalyst Summary Information	68-2
Viewing a Summary of Catalyst Interfaces, VLANs, and VLAN Groups	68-3
Interfaces	68-5
Creating or Editing Ports on Cisco Catalyst Switches and Cisco 7600 Series Routers	68-6
Deleting Ports on Cisco Catalyst Switches and Cisco 7600 Series Routers	68-7
Interfaces/VLANs Page—Interfaces Tab	68-8
Create and Edit Interface Dialog Boxes—Access Port Mode	68-9
Create and Edit Interface Dialog Boxes—Routed Port Mode	68-12
Create and Edit Interface Dialog Boxes—Trunk Port Mode	68-14
Create and Edit Interface Dialog Boxes—Dynamic Mode	68-18
Create and Edit Interface Dialog Boxes—Subinterfaces	68-22
Create and Edit Interface Dialog Boxes—Unsupported Mode	68-24

- VLANs **68-25**
 - Creating or Editing VLANs **68-26**
 - Deleting VLANs **68-27**
 - Interfaces/VLANs Page—VLANs Tab **68-27**
 - Create and Edit VLAN Dialog Boxes **68-28**
 - Access Port Selector Dialog Box **68-30**
 - Trunk Port Selector Dialog Box **68-31**
- VLAN Groups **68-31**
 - Creating or Editing VLAN Groups **68-32**
 - Deleting VLAN Groups **68-33**
 - Interfaces/VLANs Page—VLAN Groups Tab **68-33**
 - Create and Edit VLAN Group Dialog Boxes **68-34**
 - Service Module Slot Selector Dialog Box **68-35**
 - VLAN Selector Dialog Box **68-35**
- VLAN ACLs (VACLs) **68-36**
 - Creating or Editing VACLs **68-37**
 - Deleting VACLs **68-38**
 - VLAN Access Lists Page **68-39**
 - Create and Edit VLAN ACL Dialog Boxes **68-41**
 - Create and Edit VLAN ACL Content Dialog Boxes **68-41**
- IDSM Settings **68-43**
 - Creating or Editing EtherChannel VLAN Definitions **68-44**
 - Deleting EtherChannel VLAN Definitions **68-45**
 - Creating or Editing Data Port VLAN Definitions **68-46**
 - Deleting Data Port VLAN Definitions **68-47**
 - IDSM Settings Page **68-47**
 - Create and Edit IDSM EtherChannel VLANs Dialog Boxes **68-49**
 - Create and Edit IDSM Data Port VLANs Dialog Boxes **68-49**

PART 7

Monitoring, Reporting, and Diagnostics

CHAPTER 69

Viewing Events 69-1

- Introduction to Event Viewer Capabilities **69-1**
 - Historical View **69-2**
 - Real-Time View **69-2**
 - Views and Filters **69-3**
 - Policy Navigation **69-3**
 - Understanding Event Viewer Access Control **69-4**
 - Scope and Limits of Event Viewer **69-4**

Deeply Parsed Syslogs	69-6
Overview of Event Viewer	69-7
Event Viewer File Menu	69-9
Event Viewer View Menu	69-10
View List	69-12
Event Monitoring Window	69-14
Event Table Toolbar	69-16
Columns in Event Table	69-18
Time Slider	69-25
Event Details Pane	69-26
Preparing for Event Management	69-27
Ensuring Time Synchronization	69-27
Configuring ASA and FWSM Devices for Event Management	69-28
Configuring IPS Devices for Event Management	69-29
Managing the Event Manager Service	69-30
Starting, Stopping, and Configuring the Event Manager Service	69-30
Monitoring the Event Manager Service	69-31
Selecting Devices to Monitor	69-34
Monitoring Event Data Store Disk Space Usage	69-35
Archiving or Backing Up and Restoring the Event Data Store	69-36
Using Event Viewer	69-37
Using Event Views	69-37
Opening Views	69-38
Floating and Arranging Views	69-38
Customizing the Event Table Appearance	69-39
Switching Between Source/Destination IP Addresses and Host Object Names	69-39
Configuring Color Rules for a View	69-40
Creating Custom Views	69-41
Editing a Custom View Name or Description	69-41
Switching Between Real-Time and Historical Views	69-42
Saving Views	69-42
Deleting Custom Views	69-43
Filtering and Querying Events	69-43
Selecting the Time Range for Events	69-43
Using the Time Slider with Filtering	69-44
Refreshing the Event Table	69-44
Creating Column-Based Filters	69-45
Filtering Based on a Specific Event's Values	69-47
Filtering on a Text String	69-47

- Clearing Filters **69-48**
- Performing Operations on Specific Events **69-49**
 - Event Context (Right-Click) Menu **69-49**
 - IPS Signature Quick Tune Dialog Box **69-52**
 - Examining Details of a Single Event **69-53**
 - Copying Event Records **69-53**
 - Saving Events to a File **69-53**
- Looking Up a Security Manager Policy from Event Viewer **69-54**
- Looking Up Events for a Security Manager Policy **69-55**
 - Viewing Events for an Access Rule **69-56**
 - Viewing Events for an IPS Signature **69-57**
 - Viewing Events for HPM Devices and Site-to-Site VPNs **69-58**
- Examples of Event Analysis **69-58**
 - Help Desk: User Access To a Server Is Blocked By the Firewall **69-59**
 - Monitoring and Mitigating Botnet Activity **69-61**
 - Understanding the Syslog Messages That Indicate Actionable Events **69-61**
 - Monitoring Botnet Using the Security Manager Event Viewer **69-62**
 - Monitoring Botnet Using the Security Manager Report Manager **69-64**
 - Monitoring Botnet Activity Using the Adaptive Security Device Manager (ASDM) **69-64**
 - Mitigating Botnet Traffic **69-65**
 - Removing False Positive IPS Events from the Event Table **69-66**

CHAPTER 70

Managing Reports 70-1

- Understanding Report Management **70-1**
 - Understanding the Types of Reports Available in Security Manager **70-2**
 - Preparing Devices for Report Manager Reporting **70-3**
 - Understanding Report Manager Data Aggregation **70-4**
 - Understanding Report Manager Access Control **70-5**
- Overview of Report Manager **70-6**
 - Report Manager Menus **70-8**
 - Understanding the Report List in Report Manager **70-9**
 - Understanding the Report Settings Pane **70-10**
 - Understanding the Generated Report Pane and Toolbar **70-12**
- Understanding the Predefined System Reports in Report Manager **70-13**
 - Understanding Firewall Traffic Reports **70-14**
 - Understanding Firewall Summary Botnet Reports **70-15**
 - Understanding VPN Top Reports **70-16**
 - Understanding General VPN Reports **70-16**
 - Understanding IPS Top Reports **70-17**

Understanding General IPS Reports	70-19
Working with Reports in Report Manager	70-19
Opening and Generating Reports	70-20
Creating Custom Reports	70-21
Editing Report Settings	70-22
Drilling Down into Report Data	70-26
Printing Reports	70-27
Exporting Reports	70-28
Configuring Default Settings for Reports	70-29
Arranging Report Windows	70-30
Saving Reports	70-31
Renaming Reports	70-31
Closing Report Windows	70-32
Deleting Reports	70-32
Managing Custom Reports	70-32
Scheduling Reports	70-33
Viewing Report Schedules	70-33
Configuring Report Schedules	70-34
Viewing Scheduled Report Results	70-35
Enabling and Disabling Report Schedules	70-36
Deleting Report Schedules	70-36
Troubleshooting Report Manager	70-36

CHAPTER 71

Health and Performance Monitoring	71-1
Health and Performance Monitor Overview	71-1
Trend Information	71-2
Monitoring Multiple Contexts	71-3
HPM Access Control	71-3
Preparing for Health and Performance Monitoring	71-4
Launching the Health and Performance Monitor	71-4
Managing Monitored Devices	71-5
HPM Window	71-6
Working with Table Columns	71-8
Showing and Hiding Table Columns	71-8
Column-based Filtering	71-17
Using The List Filter Fields	71-19
Monitoring Devices	71-21
Managing Device Views	71-21

- Views: Opening and Closing 71-23
- Views: Tiling Horizontally or Vertically 71-23
- Views: Floating and Docking 71-24
- Views: Custom 71-24
- HPM Window: Monitoring Display 71-25
 - Monitoring Views: Devices or VPNs Summary 71-27
 - Monitoring Views: Device or VPN Status List 71-27
 - Monitoring Views: Device or VPN Details 71-28
 - Monitoring Views: VPN, RA and S2S 71-30
 - Exporting HPM Data 71-31
- Alerts and Notifications 71-32
 - HPM Window: Alerts Display 71-32
 - Alerts: Configuring 71-34
 - Alerts Configuration: IPS 71-35
 - Alerts Configuration: Firewall 71-37
 - Alerts Configuration: VPN 71-39
 - Alerts: Viewing 71-41
 - Alerts: Acknowledging and Clearing 71-42
 - Alerts: History 71-43
- SNMP Trap Forwarding Notification 71-44
 - SNMP Trap Entries Dialog Box 71-45
 - Add/Edit/Copy SNMP Trap Entries Dialog Box 71-46

CHAPTER 72

Using External Monitoring, Troubleshooting, and Diagnostic Tools 72-1

- Dashboard Overview 72-1
- CSM Mobile 72-11
- Viewing Inventory Status 72-12
 - Inventory Status Window 72-13
- Starting Device Managers 72-14
 - Troubleshooting Device Managers 72-16
 - Access Rule Look-up from Device Managers 72-17
 - Navigating to an Access Rule from ASDM 72-18
 - Navigating to an Access Rule from SDM 72-19
- Launching Cisco Prime Security Manager or FireSIGHT Management Center 72-20
 - Detecting ASA CX and FirePOWER Modules 72-21
 - Sharing Device Inventory and Policy Objects with PRSM 72-23
- Analyzing an ASA or PIX Configuration Using Packet Tracer 72-23
- Analyzing Connectivity Issues Using the Ping, Trace Route, or NS Lookup Tools 72-26
 - Analyzing Configuration Using Ping 72-27

Analyzing Configuration Using TraceRoute	72-29
Analyzing Configuration Using NS Lookup	72-30
Using the Packet Capture Wizard	72-31
IP Intelligence	72-34
Integrating CS-MARS and Security Manager	72-37
Checklist for Integrating CS-MARS with Security Manager	72-38
Configuring the Security Manager Server to Respond to CS-MARS Policy Queries	72-39
Registering CS-MARS Servers in Security Manager	72-40
Discovering or Changing the CS-MARS Controllers for a Device	72-41
Troubleshooting Tips for CS-MARS Querying	72-42
Looking Up CS-MARS Events for a Security Manager Policy	72-43
Viewing CS-MARS Events for an Access Rule	72-44
Viewing CS-MARS Events for an IPS Signature	72-46
Looking Up a Security Manager Policy from a CS-MARS Event	72-47
System Log Messages Supported for Policy Look-up	72-48
NetFlow Event Reporting in CS-MARS	72-49

PART 8**Image Management****CHAPTER 73****Using Image Manager 73-1**

Getting Started with Image Manager	73-1
Image Manager Supported Platforms and Versions	73-2
Device Configurations supported by Image Manager	73-4
Image Management for Multi-Context ASA	73-5
Image Manager Supported Image Types	73-5
Administrative Settings for Image Manager	73-6
Bootstrapping Devices for Image Manager	73-8
Working with Images	73-9
View All Images	73-10
Download Images to the Repository	73-11
Working with Bundles	73-13
Creating Bundles	73-13
View Images by Bundle	73-14
Renaming Bundles	73-15
Deleting Bundles	73-15
Deleting Images from Bundles	73-15
Working with Devices	73-16
Viewing Device Inventory	73-16
Manage Images on a Device	73-17

View Device Memory	73-18
Configuring the Image Install Location	73-19
About Image Updates on Devices Using Image Manager	73-20
Validating a Proposed Image Update on a Device	73-23
Using the Image Installation Wizard to Install Images on Devices	73-26
Install Bundled Images on Devices	73-30
Install Compatible Images on Devices	73-30
Install Images on Selected Devices	73-31
Working with Jobs	73-32
Viewing Image Installation Job Summary	73-33
Viewing Install Jobs	73-34
Aborting an Image Installation Job	73-35
Retry a Failed Image Install Job	73-35
Roll Back a Deployed Job	73-35
Image Installation Job Approval Workflow	73-36
Troubleshooting Image Management	73-37