Cisco ASA

All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance

Second Edition

Identify, mitigate, and respond to network attacks

Jazib Frahim, CCIE® No. 5459
Omar Santos

ciscopress.com

Jazib Frahim, Omar Santos

Copyright © 2010 Cisco Systems, Inc.

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

Third Printing July 2011

Library of Congress Cataloging-in-Publication data is on file.


Warning and Disclaimer

This book is designed to provide information about Cisco ASA. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.
Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact:
International Sales international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger
Associate Publisher: Dave Dusthimer
Executive Editor: Brett Bartow
Managing Editor: Patrick Kanouse
Project Editor: Seth Kerney
Book and Cover Designer: Louisa Adair
Composition: Mark Shirar
Proofreaders: Water Crest Publishing, Inc., Apostrophe Editing Services

Business Operation Manager, Cisco Press: Anand Sundaram
Manager Global Certification: Erik Ullanderson
Technical Editors: Randy Ivener, Jay Johnston
Development Editors: Kimberly Debus, Dayna Isley
Copy Editor: Margo Catts
Editorial Assistant: Vanessa Evans
Indexer: Ken Johnson
About the Authors

Jazib Frahim, CCIE No. 5459, has been with Cisco Systems for more than ten years. With a bachelor’s degree in computer engineering from Illinois Institute of Technology, he started out as a TAC engineer in the LAN Switching team. He then moved to the TAC Security team, where he acted as a technical leader for the security products. He led a team of 20 engineers in resolving complicated security and VPN technologies. He is currently working as a technical leader in the Worldwide Security Services Practice of Advanced Services for Network Security. He is responsible for guiding customers in the design and implementation of their networks with a focus on network security. He holds two CCIEs, one in routing and switching and the other in security. He has written numerous Cisco online technical documents and has been an active member on the Cisco online forum NetPro. He has presented at Networkers on multiple occasions and has taught many on-site and online courses to Cisco customers, partners, and employees.

While working for Cisco, he pursued his master of business administration (MBA) degree from North Carolina State University.

He is also an author of the following Cisco Press books:

- *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*
- *Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting*
- *SSL Remote Access VPNs*

Omar Santos is an incident manager at Cisco’s Product Security Incident Response Team (PSIRT). Omar has designed, implemented, and supported numerous secure networks for Fortune 500 companies and the U.S. government, including the United States Marine Corps (USMC) and the U.S. Department of Defense (DoD). He is also the author of many Cisco online technical documents and configuration guidelines. Prior to his current role, he was a technical leader within the World Wide Security Practice and Cisco’s Technical Assistance Center (TAC), where he taught, led, and mentored many engineers within both organizations.

Omar has also delivered numerous technical presentations to Cisco customers and partners; as well as executive presentations to CEOs, CIOs, and CSOs of many organizations. He is also the author of the following Cisco Press books:

- *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*
- *Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting*
- *End-to-End Network Security: Defense-in-Depth*
About the Technical Reviewers

**Randy Ivener**, CCIE No. 10722, is a security engineer in the Cisco Security Research and Operations team. He is a CISSP and PMI PMP. He has spent many years as a network security consultant helping companies understand and secure their networks. Randy has presented security topics at industry events including Blackhat and Cisco Networkers. Before becoming immersed in information security, he spent time in software development and as a training instructor. Randy graduated from the U.S. Naval Academy and holds an MBA.

**Jay Johnston**, CCIE No. 17663, is a security specialist in the Cisco TAC center located in Research Triangle Park, North Carolina. His networking career began in 2002 when he joined Cisco as a co-op while attending North Carolina State University. After graduating with a bachelors of computer science in 2004, he joined Cisco full time as a TAC Engineer. He obtained his Security CCIE in 2007. He enjoys working for Cisco, especially the constant technical challenges that working with customers in the TAC provides.
Dedications

Jazib Frabim: I would like to dedicate this book to my lovely wife, Sadaf, who has patiently put up with me during the writing process.

I would also like to dedicate this book to my parents, Frahim and Perveen, who support and encourage me in all my endeavors.

Finally, I would like to thank my siblings, including my brother Shazib and sisters Erum and Sana, sister-in-law Asiya, my cute nephew Shayan, and my adorable nieces Shiza and Alisha. Thank you for your patience and understanding during the development of this book.

Omar Santos: I would like to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book.

I also dedicate this book to my parents, Jose and Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.

Acknowledgments

We would like to thank the technical editors, Randy Ivener and Jay Johnston, for their time and technical expertise. They verified our work and corrected us in all the major and minor mistakes that were hard to find. Special thanks go to Aun Raza for reviewing many chapters prior to final editing.

We would like to thank the Cisco Press team, especially Brett Bartow, Dayna Isley, Kimberley Debus, and Andrew Cupp for their patience, guidance, and consideration. Their efforts are greatly appreciated.

Many thanks to our Cisco management team, including David Philips, Ken Cavanagh, and Jean Reese for their continuous support. They highly encouraged us throughout this project.

Kudos to the Cisco ASA product development team for delivering such a great product. Their support is also greatly appreciated during the development of this book.

Finally, we would like to acknowledge the Cisco TAC. Some of the best and brightest minds in the networking industry work there, supporting our Cisco customers often under very stressful conditions and working miracles daily. They are truly unsung heroes, and we are all honored to have had the privilege of working side by side with them in the trenches of the TAC.
Contents at a Glance

Introduction xxiii

Part I: Product Overview
Chapter 1 Introduction to Security Technologies 1
Chapter 2 Cisco ASA Product and Solution Overview 25
Chapter 3 Initial Setup and System Maintenance 49

Part II: Firewall Technology
Chapter 4 Controlling Network Access 141
Chapter 5 IP Routing 231
Chapter 6 Authentication, Authorization, and Accounting (AAA) 311
Chapter 7 Application Inspection 349
Chapter 8 Virtualization 415
Chapter 9 Transparent Firewalls 474
Chapter 10 Failover and Redundancy 521
Chapter 11 Quality of Service 577

Part III: Intrusion Prevention System (IPS) Solutions
Chapter 12 Configuring and Troubleshooting Intrusion Prevention System (IPS) 615
Chapter 13 Tuning and Monitoring IPS 677

Part IV: Content Security
Chapter 14 Configuring Cisco Content Security and Control Security Services Module 689
Chapter 15 Monitoring and Troubleshooting the Cisco Content Security and Control Security Services Module 715

Part V: Virtual Private Network (VPN) Solutions
Chapter 16 Site-to-Site IPSec VPNs 735
Chapter 17 IPSec Remote-Access VPNs 799
Chapter 18 Public Key Infrastructure (PKI) 869
Chapter 19 Clientless Remote-Access SSL VPNs 923
Chapter 20 Client-Based Remote-Access SSL VPNs 1027

Index 1067
Contents

Introduction xxiii

Part I: Product Overview

Chapter 1 Introduction to Security Technologies 1

Firewalls 1

Network Firewalls 2
Stateful Inspection Firewalls 6
Deep Packet Inspection 7
Personal Firewalls 7

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) 8

Pattern Matching and Stateful Pattern-Matching Recognition 9
Protocol Analysis 10
Heuristic-Based Analysis 11
Anomaly-Based Analysis 11

Virtual Private Networks 12

Technical Overview of IPSec 14
SSL VPNs 21

Summary 23

Chapter 2 Cisco ASA Product and Solution Overview 25

Cisco ASA 5505 Model 26
Cisco ASA 5510 Model 29
Cisco ASA 5520 Model 34
Cisco ASA 5540 Model 36
Cisco ASA 5550 Model 36
Cisco ASA 5580-20 and 5580-40 Models 38

Cisco ASA 5580-20 39
Cisco ASA 5580-40 40

Cisco ASA AIP-SSM Module 41
Cisco ASA AIP-SSM-10 43
Cisco ASA AIP-SSM-20 43
Cisco ASA AIP-SSM-40 43

Cisco ASA Gigabit Ethernet Modules 44
Cisco ASA 4GE-SSM 44

Cisco ASA 5580 Expansion Cards 45

Cisco ASA CSC-SSM Module 46

Summary 47
Chapter 3  Initial Setup and System Maintenance  49

Accessing the Cisco ASA Appliances  49
  Establishing a Console Connection  50
  Command-Line Interface  52

Managing Licenses  54

Initial Setup  57
  Initial Setup via CLI  57
  Initial Setup of ASDM  58

Device Setup  67
  Setting Up Device Name and Passwords  67
  Configuring an Interface  69
  DHCP Services  76

IP Version 6  78
  IPv6 Header  78
  Configuring IPv6  80

Setting Up the System Clock  84
  Manual Clock Adjustment  84
  Automatic Clock Adjustment Using the Network Time Protocol  86

Configuration Management  88
  Running Configuration  88
  Startup Configuration  92
  Removing the Device Configuration  93

Remote System Management  94
  Telnet  95
  Secure Shell (SSH)  98

System Maintenance  101
  Software Installation  101
  Password Recovery Process  106
  Disabling the Password Recovery Process  109

System Monitoring  113
  System Logging  113
  NetFlow Secure Event Logging (NSEL)  125
  Simple Network Management Protocol (SNMP)  128

Device Monitoring and Troubleshooting  133
  CPU and Memory Monitoring  133
  Troubleshooting Device Issues  136

Summary  139
Part II: Firewall Technology

Chapter 4  Controlling Network Access  141

Packet Filtering  141
  Types of ACLs  144
  Comparing ACL Features  146

Configuring Traffic Filtering  147
  Thru-Traffic Filtering via CLI  147
  Thru-Traffic Filtering via ASDM  152
  To-The-Box-Traffic Filtering  154
  Set Up an IPv6 ACL (Optional)  157

Advanced ACL Features  159
  Object Grouping  159
  Standard ACLs  166
  Time-Based ACLs  167
  Downloadable ACLs  170
  ICMP Filtering  172

Content and URL Filtering  173
  Content Filtering  173
  URL Filtering  175

Deployment Scenarios for Traffic Filtering  185
  Using ACLs to Filter Inbound Traffic  185
  Using Websense to Enable Content Filtering  190

Monitoring Network Access Control  193
  Monitoring ACLs  193
  Monitoring Content Filtering  198

Understanding Address Translation  199
  Network Address Translation  200
  Port Address Translation  202
  Address Translation and Interface Security Levels  203
  Packet Flow Sequence  204
  Security Protection Mechanisms Within Address Translation  204

Configuring Address Translation  206
  Bypassing Address Translation  218
  NAT Order of Operation  222
  Integrating ACLs and NAT  223

DNS Doctoring  225
  Monitoring Address Translations  229

Summary  230
Chapter 5  IP Routing  231
  Configuring Static Routes  231
  Static Route Monitoring  234
  Displaying the Routing Table  239
  RIP  240
  Configuring RIP  241
  RIP Authentication  244
  RIP Route Filtering  246
  Configuring RIP Redistribution  249
  Troubleshooting RIP  249
  OSPF  252
  Configuring OSPF  254
  Troubleshooting OSPF  272
  EIGRP  280
  Configuring EIGRP  280
  Troubleshooting EIGRP  292
  IP Multicast  301
  IGMP Stub Mode  301
  PIM Sparse Mode  301
  Configuring Multicast Routing  302
  Troubleshooting IP Multicast Routing  308
  Summary  310

Chapter 6  Authentication, Authorization, and Accounting (AAA)  311
  AAA Protocols and Services Supported by Cisco ASA  312
    RADIUS  314
    TACACS+  316
    RSA SecurID  316
    Microsoft Windows NT  317
    Active Directory and Kerberos  318
    Lightweight Directory Access Protocol  318
    HTTP Form Protocol  318
  Defining an Authentication Server  318
  Configuring Authentication of Administrative Sessions  325
    Authenticating Telnet Connections  325
    Authenticating SSH Connections  327
    Authenticating Serial Console Connections  329
    Authenticating Cisco ASDM Connections  329
HTTP 390
   Enabling HTTP Inspection 391
ICMP 399
ILS 399
Instant Messenger (IM) 400
IPSec Pass-Through 403
MGCP 404
NetBIOS 406
PPTP 406
Sun RPC 407
SSH 407
RTSP 408
SIP 408
Skinny (SCCP) 410
SNMP 411
SQL*Net 412
TFTP 412
WAAS 413
XDMCP 413
Summary 413

Chapter 8 Virtualization 415

   Architectural Overview 417
      System Execution Space 417
      Admin Context 418
      User Context 419
   Packet Classification 421
      Packet Flow in Multiple Mode 424
   Configuration of Security Contexts 427
      Step 1: Enable Multiple Security Contexts Globally 427
      Step 2: Set Up the System Execution Space 430
      Step 3: Allocate Interfaces 433
      Step 4: Specify a Configuration URL 434
      Step 5: Configure an Admin Context 435
      Step 6: Configure a User Context 437
      Step 7: Manage the Security Contexts (Optional) 438
      Step 8: Resource Management (Optional) 439
Deployment Scenarios 443

Virtual Firewalls That Use Non-Shared Interfaces 443
Virtual Firewalls That Use a Shared Interface 454

Monitoring and Troubleshooting the Security Contexts 466
Monitoring 466
Troubleshooting 468

Summary 470

Chapter 9  Transparent Firewalls 471

Architectural Overview 474
Single-Mode Transparent Firewalls 474
Multimode Transparent Firewalls 477

Restrictions Within Transparent Firewalls 478
Transparent Firewalls and VPNs 479
Transparent Firewalls and NAT 479

Configuration of Transparent Firewalls 482
Configuration Guidelines 482
Configuration Steps 483

Deployment Scenarios 496
SMTF Deployment 496
MMTF Deployment with Security Contexts 502

Monitoring and Troubleshooting the Transparent Firewalls 514
Monitoring 514
Troubleshooting 516

Summary 519

Chapter 10  Failover and Redundancy 521

Architectural Overview 521
Conditions that Trigger Failover 523
Failover Interface Tests 523
Stateful Failover 524

Hardware and Software Requirements 525
Types of Failover 527
Interface-Level Failover 531

Failover Configuration 533
Device-Level Redundancy Configuration 533
ASDM Failover Wizard Configuration 548
Interface Level Redundancy Configuration 550
Optional Failover Commands 552
Zero-Downtime Software Upgrade 557
Deployment Scenarios 559
Active/Standby Failover in Single Mode 560
Active/Active Failover in Multiple Security Contexts 564
Monitoring and Troubleshooting Failovers 569
Monitoring 569
Troubleshooting 572
Summary 575

Chapter 11 Quality of Service 577
QoS Types 579
Traffic Prioritization 579
Traffic Policing 579
Traffic Shaping 581
QoS Architecture 582
Packet Flow Sequence 582
Packet Classification 583
QoS and VPN Tunnels 587
Configuring Quality of Service 588
QoS Configuration via ASDM 589
QoS Configuration via CLI 596
QoS Deployment Scenarios 600
QoS for VoIP Traffic 600
QoS for the Remote-Access VPN Tunnels 607
Monitoring QoS 611
Summary 613

Part III: Intrusion Prevention System (IPS) Solutions

Chapter 12 Configuring and Troubleshooting Intrusion Prevention System (IPS) 615
Overview of the Adaptive Inspection Prevention Security Services Module (AIP-SSM) and Adaptive Inspection Prevention Security Services Card (AIP-SSC) 615
AIP-SSM and AIP-SSC Management 616
Inline Versus Promiscuous Mode 617
Cisco IPS Software Architecture 619
MainApp 620
SensorApp 621
Attack Response Controller 622
AuthenticationApp 623
cipsWebserver 623
Logger 624
EventStore 624
CtlTransSource 625
Configuring the AIP-SSM 625
Introduction to the CIPS CLI 625
User Administration 632
AIP-SSM Maintenance 636
Adding Trusted Hosts 636
Upgrading the CIPS Software and Signatures 637
Displaying Software Version and Configuration Information 643
Backing Up Your Configuration 647
Displaying and Clearing Events 648
Advanced Features and Configuration 650
Custom Signatures 651
IP Logging 656
Configuring Blocking (Shunning) 659
Cisco Security Agent Integration 662
Anomaly Detection 666
Cisco ASA Botnet Detection 670
Dynamic and Administrator Blacklist Data 670
DNS Snooping 672
Traffic Classification 672
Summary 675

Chapter 13 Tuning and Monitoring IPS 677
IPS Tuning 677
Disabling IPS Signatures 679
Retiring IPS Signatures 680
Monitoring and Tuning the AIP-SSM Using CS-MARS 681
Adding the AIP-SSM in CS-MARS 682
Tuning the AIP-SSM Using CS-MARS 683
Displaying and Clearing Statistics 684
Summary 688

Part IV: Content Security

Chapter 14 Configuring Cisco Content Security and Control Security Services Module 689
Initial CSC SSM Setup 690
Chapter 15 Monitoring and Troubleshooting the Cisco Content Security and
Control Security Services Module  715

Monitoring the CSC SSM  715
  Detailed Live Event Monitoring  717
  Configuring Syslog  718
Troubleshooting the CSC SSM  719
  Re-Imaging the CSC SSM  719
  Password Recovery  722
  Configuration Backup  724
  Upgrading the CSC SSM Software  726
  CLI Troubleshooting Tools  726
Summary  734

Part V: Virtual Private Network (VPN) Solutions

Chapter 16 Site-to-Site IPSec VPNs  735

Preconfiguration Checklist  736
Configuration Steps  738
  Step 1: Enable ISAKMP  739
  Step 2: Create the ISAKMP Policy  739
  Step 3: Set Up the Tunnel Groups  741
  Step 4: Define the IPSec Policy  743
  Step 5: Create a Crypto Map  745
  Step 6: Configure Traffic Filtering (Optional)  749
  Step 7: Bypass NAT (Optional)  751
Alternate Configuration Methods Through ASDM  752
Advanced Features 754
  OSPF Updates over IPSec 755
  Reverse Route Injection 757
  NAT Traversal 758
  Tunnel Default Gateway 759
  Management Access 760
  Perfect Forward Secrecy 761
Modifying Default Parameters 762
  Security Association Lifetimes 763
  Phase 1 Mode 764
  Connection Type 764
  ISAKMP Keepalives 766
  IPSec and Packet Fragmentation 767
Deployment Scenarios 768
  Single Site-to-Site Tunnel Configuration Using NAT-T 769
  Fully Meshed Topology with RRI 775
Monitoring and Troubleshooting Site-to-Site IPSec VPNS 789
  Monitoring Site-to-Site VPNS 789
  Troubleshooting Site-to-Site VPNS 793
Summary 798

Chapter 17  IPSec Remote-Access VPNS 799
Cisco IPSec Remote Access VPN Solution 800
  IPSec Remote-Access Configuration Steps 801
  Step 2: Create the ISAKMP Policy 803
  Step 3: Set Up Tunnel and Group Policies 805
  Step 4: Define the IPSec Policy 809
  Step 5: Configure User Authentication 810
  Step 6: Assign an IP Address 812
  Step 7: Create a Crypto Map 816
  Step 8: Configure Traffic Filtering (Optional) 817
  Step 9: Bypass NAT (Optional) 818
  Step 10: Set Up Split Tunneling (Optional) 818
  Step 11: Assign DNS and WINS (Optional) 821
  Alternate Configuration Method through ASDM 822
Cisco VPN Client Configuration 824
Advanced Cisco IPSec VPN Features 828
  Tunnel Default Gateway 828
  Transparent Tunneling 829
  IPSec Hairpinning 831
  VPN Load Balancing 833
  Client Firewalling 836
  Hardware-Based Easy VPN Client Features 840
L2TP Over IPSec Remote Access VPN Solution 843
  L2TP over IPSec Remote-Access Configuration Steps 845
  Windows L2TP over IPSec Client Configuration 848
Deployment Scenarios 849
  Load Balancing of Cisco IPSec Clients and Site-to-Site Integration 849
  L2TP over IPSec with Traffic Hairpinning 855
Monitoring and Troubleshooting Cisco Remote-Access VPN 860
  Monitoring Cisco Remote Access IPSec VPNs 860
  Troubleshooting Cisco IPSec VPN Clients 865
Summary 868

Chapter 18 Public Key Infrastructure (PKI) 869
Introduction to PKI 869
  Certificates 870
  Certificate Authority (CA) 871
  Certificate Revocation List 873
  Simple Certificate Enrollment Protocol 874
Installing Certificates 874
  Installing Certificates Through ASDM 874
  Installing Certificates Using the CLI 883
The Local Certificate Authority 896
  Configuring the Local CA Through ASDM 896
  Configuring the Local CA Using the CLI 899
  Enrolling Local CA Users Through ASDM 901
  Enrolling Local CA Users Through the CLI 904
Configuring IPSec Site-to-Site Tunnels Using Certificates 906
Configuring the Cisco ASA to Accept Remote-Access IPSec VPN Clients
  Using Certificates 910
  Enrolling the Cisco VPN Client 911
  Configuring the Cisco ASA 914
Troubleshooting PKI  917
   Time and Date Mismatch  917
   SCEP Enrollment Problems  920
   CRL Retrieval Problems  921
Summary  922

Chapter 19  Clientless Remote-Access SSL VPNs  923

SSL VPN Design Considerations  924
   User Connectivity  924
   ASA Feature Set  925
   Infrastructure Planning  925
   Implementation Scope  925
SSL VPN Prerequisites  926
   SSL VPN Licenses  926
   Client Operating System and Browser and Software Requirements  930
   Infrastructure Requirements  931
Pre-SSL VPN Configuration Guide  931
   Enroll Digital Certificates (Recommended)  931
   Set Up Tunnel and Group Policies  937
   Set Up User Authentication  943
Clientless SSL VPN Configuration Guide  947
   Enable Clientless SSL VPN on an Interface  949
   Configure SSL VPN Portal Customization  949
   Configure Bookmarks  965
   Configure Web-Type ACLs  970
   Configure Application Access  973
   Configure Client-Server Plug-ins  979
Cisco Secure Desktop  980
   CSD Components  981
   CSD Requirements  983
   CSD Architecture  984
   Configuring CSD  985
Host Scan  998
   Host Scan Modules  999
   Configuring Host Scan  1000
Dynamic Access Policies  1003
   DAP Architecture  1004
Icons Used in This Book

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a `show` command).

- **Italic** indicates arguments for which you supply actual values.

- Vertical bars (|) separate alternative, mutually exclusive elements.

- Square brackets ([ ]) indicate an optional element.

- Braces ({ }) indicate a required choice.

- Braces within brackets ({[ ]}) indicate a required choice within an optional element.
Introduction

Network security has always been a challenge for many organizations that cannot deploy separate devices to provide firewall, intrusion prevention, and virtual private network (VPN) services. The Cisco ASA is a high-performance, multifunction security appliance that offers firewall, IPS, network antivirus, and VPN services. The Cisco ASA delivers these features through improved network integration, resiliency, and scalability.

This book is an insider's guide to planning, implementing, configuring, and troubleshooting the Cisco Adaptive Security Appliances. It delivers expert guidance from senior Cisco network security consulting engineers. It demonstrates how adaptive identification and mitigation services on the Cisco ASA provide a sophisticated network security solution to small, medium, and large organizations. This book brings together expert guidance for virtually every challenge you will face—from building basic network security policies to advanced VPN and IPS implementations.

Who Should Read This Book?

This book serves as a guide for any network professional who manages network security or installs and configures firewalls, VPN devices, or intrusion detection/prevention systems. It encompasses topics from an introductory level to advanced topics on security and VPNs. The requirements of the reader include a basic knowledge of TCP/IP and networking.

How This Book Is Organized

This book has five parts, which provide a Cisco ASA product introduction and then focus on firewall features, intrusion prevention, content security, and VPNs. Each part includes many sample configurations, accompanied by in-depth analyses of design scenarios. Your learning is further enhanced by a discussion of a set of debugs included in each technology. Ground-breaking features, such as SSL VPN and virtual and Layer 2 firewalls, are discussed extensively.

The core chapters, Chapters 2 through 12, cover the following topics:

- Part I, “Product Overview,” includes the following chapters:
  - Chapter 1, “Introduction to Security Technologies”—This chapter provides an overview of different technologies that are supported by the Cisco ASA and widely used by today’s network security professionals.
  - Chapter 2, “Cisco ASA Product and Solution Overview”—This chapter describes how the Cisco ASA incorporates features from each of these products, integrating comprehensive firewall, intrusion detection and prevention, and VPN technologies in a cost-effective, single-box format. Additionally, it provides a hardware overview of the Cisco ASA, including detailed technical specifications and installation guidelines. It also covers an overview of the Adaptive Inspection and Prevention Security Services Module (AIP-SSM) and Content Security and Control Security Services Module (CSC-SSM).
Chapter 3, “Initial Setup and System Maintenance”—A comprehensive list of initial setup tasks and system maintenance procedures is included in this chapter. These tasks and procedures are intended to be used by network professionals who will be installing, configuring, and managing the Cisco ASA.

Part II, “Firewall Technology,” includes the following chapters:

- Chapter 4, “Controlling Network Access”—The Cisco ASA can protect one or more networks from intruders. Connections between these networks can be carefully controlled by advanced firewall capabilities, enabling you to ensure that all traffic from and to the protected networks passes only through the firewall based on the organization’s security policy. This chapter shows you how to implement your organization’s security policy, using the features the Cisco ASA provides.

- Chapter 5, “IP Routing”—This chapter covers the different routing capabilities of the Cisco ASA.

- Chapter 6, “Authentication, Authorization, and Accounting (AAA)”—The Cisco ASA supports a wide range of AAA features. This chapter provides guidelines on how to configure AAA services by defining a list of authentication methods applied to various implementations.

- Chapter 7, “Application Inspection”—The Cisco ASA stateful application inspection helps to secure the use of applications and services in your network. This chapter describes how to use and configure application inspection.

- Chapter 8, “Virtualization”—The Cisco ASA virtual firewall feature introduces the concept of operating multiple instances of firewalls (contexts) within the same hardware platform. This chapter shows how to configure and troubleshoot each of these security contexts.

- Chapter 9, “Transparent Firewalls”—This chapter introduces the transparent (Layer 2) firewall model within the Cisco ASA. It explains how users can configure the Cisco ASA in transparent single mode and multiple mode while accommodating their security needs.

- Chapter 10, “Failover and Redundancy”—This chapter discusses the different redundancy and failover mechanisms that the Cisco ASA provides. It includes not only the overview and configuration, but also detailed troubleshooting procedures.

- Chapter 11, “Quality of Service”—QoS is a network feature that lets you give priority to certain types of traffic. This chapter covers how to configure and troubleshoot QoS in the Cisco ASA.

Part III, “Intrusion Prevention System (IPS) Solutions,” includes the following chapters:

- Chapter 12, “Configuring and Troubleshooting Intrusion Prevention System (IPS)”—Intrusion detection and prevention systems provide a level of protection beyond the firewall by securing the network against internal and external
attacks and threats. This chapter describes the integration of Intrusion Prevention System (IPS) features within the Cisco ASA and expert guidance on how to configure the AIP-SSM IPS software. Troubleshooting scenarios are also included to enhance learning.

- Chapter 13, “Tuning and Monitoring IPS”—This chapter covers the IPS tuning process, as well as best practices on how to monitor IPS events.

Part IV, “Content Security,” includes the following chapters:

- Chapter 14, “Configuring Cisco Content Security and Control Security Services Module”—The Content Security and Control Security Services Module (CSC-SSM) is used to detect and take action on viruses, worms, Trojans, and other security threats. It supports the inspection of SMTP, POP3, HTTP, and FTP network traffic. This chapter provides configuration and troubleshooting guidelines to successfully deploy the CSC-SSM within your organization.

- Chapter 15, “Monitoring and Troubleshooting the Cisco Content Security and Control Security Services Module”—This chapter provides best practices and methodologies used while monitoring the CSC-SSM and troubleshooting any problems you may encounter.

Part V, “Virtual Private Network (VPN) Solutions,” includes the following chapters:

- Chapter 16, “Site-to-Site IPSec VPNs”—The Cisco ASA supports IPSec VPN features that enable you to connect networks in different geographic locations. This chapter provides configuration and troubleshooting guidelines to successfully deploy site-to-site IPSec VPNs.

- Chapter 17, “IPSec Remote-Access VPNs”—This chapter discusses two IPSec remote-access VPN solutions (Cisco IPSec and L2TP over IPSec) that are supported on the Cisco ASA. A large number of sample configurations and troubleshooting scenarios are provided.

- Chapter 18, “Public Key Infrastructure (PKI)” —This chapter starts by introducing PKI concepts. It then covers the configuration and troubleshooting of PKI in the Cisco ASA.

- Chapter 19, “Clientless Remote-Access SSL VPNs”—This chapter provides details about the Clientless SSL VPN functionality in Cisco ASA. This chapter covers the Cisco Secure Desktop (CSD) solution in detail and also discusses the Host Scan feature that is used to collect posture information about end-workstations. The dynamic access policy (DAP) feature, its usage, and detailed configuration examples are also provided. To reinforce learning, many different deployment scenarios are presented along with their configurations.

- Chapter 20, “Client-Based Remote-Access SSL VPNs”—This chapter provides details about the AnyConnect SSL VPN functionality in Cisco ASA.
This page intentionally left blank
This chapter covers the following topics:

- Accessing the Cisco ASA appliances
- Managing licenses
- Initial setup
- IP version 6
- Setting up the system clock
- Configuration management
- Remote system management
- System maintenance
- System monitoring

Cisco Adaptive Security Appliance (ASA) can be set up in a number of ways to adapt to any network topology. However, proper planning is essential for successful implementations of the security features that Cisco ASA offers. This chapter guides you through the initial configuration of the security appliance and shows ways to monitor the system’s health and status.

**Accessing the Cisco ASA Appliances**

Cisco ASA provides two types of user interfaces:

- **Command-line interface (CLI)**—The CLI provides non-graphical access to the Cisco ASA. The CLI can be accessed from a console, Telnet, or Secure Shell (SSH) session. Telnet and SSH are discussed later in the chapter, under “Remote System Management.”
Graphical user interface (GUI) via ASDM—Cisco Adaptive Security Device Manager (ASDM) provides an easy-to-navigate and simple graphical interface to set up and manage the different features that Cisco Adaptive Security Appliance (ASA) provides. It is bundled with a variety of administration and monitoring tools to check the health of the appliance and the traffic traversing through it. ASDM access requires IP connectivity between the ASDM client and the security appliance. If you have a new security appliance, you can assign the initial IP address via the CLI and then establish a GUI ASDM connection.

Establishing a Console Connection

A new security appliance, by default, has no configuration and thus it does not have IP addresses assigned to any of its interfaces. To access the CLI, you need a successful connection to the console port of the security appliance. The console port is a serial asynchronous port with the settings listed in Table 3-1.

You can connect the console port on the security appliance to a serial port on a PC by using a flat rolled console cable, with a DB9 serial adapter on one end and a RJ-45 port on the other. The DB9 side of the cable goes to the serial port of a PC, and the RJ-45 end of the cable goes to the console port of the security appliance, as illustrated in Figure 3-1.

![Figure 3-1 Console Port Connectivity from a Computer](image)

After connecting the console cable to the security appliance and the computer, launch terminal-emulation software, such as HyperTerminal or TeraTerm, to send and receive output. You can launch HyperTerminal by navigating to Start > Programs > Accessories > Communications > HyperTerminal on a Windows-based PC. The initial configuration window of HyperTerminal is shown in Figure 3-2. In the Connection Description dialog box, enter a connection name to identify this session as a unique connection. A connection name of Console Connection to the Cisco ASA is specified in Figure 3-2. You can choose an icon to associate with the connection entry. After filling out the connection name and selecting an icon, click OK to proceed.
Specify the connection type in the Connect To window. Because the console port uses an asynchronous serial connection, the HyperTerminal setting must use a COM port. As illustrated in Figure 3-3, COM3 is being set up for the serial connection to the security appliance. After you are finished, click OK to proceed to the next configuration window.

**Table 3-1**  
Console Port Settings

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud rate</td>
<td>9600</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Flow control</td>
<td>Hardware</td>
</tr>
</tbody>
</table>
The last window is used to configure port properties, such as the baud rate and flow control. Figure 3-4 shows HyperTerminal set up with the values listed in Table 3-1. After configuring the port settings, click OK to complete the configuration setup.

![HyperTerminal Port Specification](image)

**Figure 3-4  Setting HyperTerminal Port Specification**

The HyperTerminal application is ready to transmit and receive data from the security appliance. If you press Enter a couple of times, you should see a ciscoasa> prompt in the HyperTerminal window.

The next section describes how to use the CLI after establishing a successful console connection.

**Command-Line Interface**

After a successful console connection, the security appliance is ready to accept your commands. The Cisco ASA contains a command set structure similar to that of a Cisco IOS router and offers the following access modes:

- User mode, also known as user access mode
- Privileged mode
- Configuration mode
- Sub-configuration mode
- ROMMON mode

*User mode*, shown as the hostname with a > sign, is the first mode of access available when you log in to the security appliance. This mode offers a limited set of commands that
are useful in obtaining basic information about the security appliance. One of the important commands in this mode is `enable`, which prompts a user to specify a password to log in to privileged mode.

*Privileged mode*, shown as the hostname with a # sign, gives full access to a user after a successful logon. This mode also allows execution of all the commands that are available in user mode. The security appliance offers a rich set of monitoring and troubleshooting commands to check the health of different processes and features in the security appliance. One of the important commands in this mode is `configure terminal`, which places a user in configuration mode.

**Note** The security appliance enables you to restrict the commands a user can run by implementing command authorization. This is covered in Chapter 6, “Authentication, Authorization, and Accounting (AAA) Services.”

*Configuration mode*, displayed as the host name with a (config)# prompt, allows a user to enable or disable a feature, set up security and networking components, and tweak the default parameters. This mode not only enables the user to configure the security appliance, but also allows the use of all the commands that are available in the user and privileged modes. A user may enter into the sub-configuration mode of different features from this mode.

*Sub-configuration mode*, displayed as the hostname with a (config-xx)# prompt, lets a user configure specific networking or security features on the security appliance. The xx is replaced by the process/feature keyword that is being configured on the security appliance. For example, if a user is setting up specific parameters on an interface, the prompt changes to (config-if)#. Sub-configuration mode enables the user to execute all the configuration mode commands as well as the user and privileged mode commands.

In Example 3-1, a user logs in to privileged mode from user access mode by typing the `enable` command. The security appliance prompts a user to specify a password to gain privileged mode access. If the security appliance has the default configuration, it uses a null (no) password to grant access. After logging in to privileged mode, the user types `configure terminal` to access configuration mode. The user enters into interface sub-configuration mode by typing the `interface GigabitEthernet0/0` command. To go back to the previous mode, the user can enter `exit` or `quit`, as shown in Example 3-1.

**Example 3-1  Accessing the Privileged and Configuration Modes**

```
ciscoasa> enable
Password: <cr>
ciscoasa# configure terminal

ciscoasa(config)# interface GigabitEthernet0/0

ciscoasa(config-if)# exit

ciscoasa(config)# exit

ciscoasa#
```
Tip  In the preceding example, the administrator of the security appliance typed exit twice to return to the privileged mode prompt. Optionally, you can type end to return to privileged mode from any configuration mode.

Like a Cisco IOS router, the security appliance also allows you to press the Tab key to complete a partial command. For example, to enter a show command, type sho and press the Tab key. The security appliance displays the complete show command on the screen.

The security appliance allows you to abbreviate commands and keywords to the number of characters that identify a distinct abbreviation. For example, you can abbreviate the enable command as en.

All the supported options and arguments of a command are displayed when you type ? after the command. For example, you can type show ? to see all the options that are supported under the show command.

The security appliance also provides a brief description and command syntax when you type help followed by the command. For example, when you type help reload, the security appliance shows the command syntax for reload, a description, and the supported arguments.

The security appliance uses ROMMON mode (Read-Only-Memory Monitor mode) when it does not find a bootable image or when an administrator forces it to enter into that mode. In ROMMON mode, you can use a TFTP server to load a system image into the security appliance. ROMMON mode is also used to recover the system password, discussed later in this chapter under “Image Recovery Using ROMMON.”

Managing Licenses

As mentioned in Chapter 2, “Cisco ASA Product and Solution Overview,” the security appliance controls the security and networking features through the use of a license key. You can obtain the information of the currently installed license key by issuing the show version command. This command also displays other system information, such as:

- The current version and the location of the system image
- The ASDM version, if installed
- The security appliance uptime
- The security appliance hardware model number, including the memory and flash information
- The physical interface and the associated IRQs (Interrupt Requests)
- The current features that are active on the security appliance
- The license information
- The security appliance’s serial number
- Configuration register setting
- Information about last configuration modification

Example 3-2 shows the output of `show version`, which has a VPN Plus–based license key installed.

**Example 3-2  Output of show version**

```
Chicago> show version
Cisco Adaptive Security Appliance Software Version 8.2(1)
Device Manager Version 6.2(1)

Compiled on Tue 05-May-09 22:45 by builders
System image file is "disk0:/asa821-k8.bin"
Config file at boot was "startup-config"

Chicago up 31 days 4 hours

Hardware: ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 64MB
BIOS Flash M50FW016 @ 0xffe00000, 2048KB

Encryption hardware device: Cisco ASA-55x0 on-board accelerator (revision 0x0)
  Boot microcode : &#x263B;CN1000-MC-BOOT-2.00
  SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
  IPSec microcode : &x263A;CNlite-MC-IPSECm-MAIN-2.04

  0: Ext: GigabitEthernet0/0 : address is 000f.f775.4b54, irq 9
  1: Ext: GigabitEthernet0/1 : address is 000f.f775.4b55, irq 9
  2: Ext: GigabitEthernet0/2 : address is 000f.f775.4b56, irq 9
  3: Ext: GigabitEthernet0/3 : address is 000f.f775.4b57, irq 9
  4: Ext: Management0/0 : address is 000f.f775.4b53, irq 11
  5: Int: Internal-Data0/0 : address is 0000.0001.0002, irq 11
  6: Int: Internal-Control0/0 : address is 0000.0001.0001, irq 5

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 150
Inside Hosts : Unlimited
Failover : Active/Active
VPN-DES : Enabled
VPN-3DES-AES : Enabled
Security Contexts : 10
GTP/GPRS : Enabled
```
In Example 3-2, the security appliance is running a system image of 8.2(1) with the ASDM image of 6.2(1). The hardware model is ASA5520, running the Plus license. The serial number and the license activation key are masked to protect this system's identity. The configuration register is set to 0x1, which instructs the security appliance to load the image from flash. The configuration register is discussed later in the “Password Recovery Process” section.

You can change the installed license key by using the `activation-key` command followed by the five-tuple key, as shown in Example 3-3. After the new activation key is entered, the security appliance shows the features set activated by the new license key. In this example, a VPN premium license key is installed.

**Example 3-3  Changing the Activation Key**

```
Chicago# activation-key 0x11223344 0x55667788 0x9900aabb 0xccddeeff 0x01234567

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs               : 100
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Security Contexts           : 50
GTP/GPRS                    : Disabled
VPN Peers                   : 5000
```

This machine has a VPN Premium license.
Both running and flash activation keys were updated with the requested key.

**Note** Feature-specific activation keys are discussed in their respective chapters. For example, Chapter 19 discusses the license model for SSL VPN tunnels.

### Initial Setup

If you are setting up a new security appliance, it must be configured from the CLI first. You cannot use ASDM until the security appliance is configured with the appropriate IP addresses and it has IP connectivity to ASDM client machine.

### Initial Setup via CLI

When the security appliance is booted with no configuration, it offers a setup menu that enables you to configure the initial parameters such as the device name and the IP address. You can choose to go through the initial setup menu for quick configuration.

In Example 3-4, a security appliance prompts users to specify whether they wish to go through the interactive menu to preconfigure the device. If a user types `no`, the interactive menu is not shown and the security appliance shows the `ciscoasa>` prompt. If a user types `yes`, the default option, the security appliance walks the user through the configuration of ten parameters. The security appliance shows the default values in brackets ([]) before prompting the user to accept or change them. To accept the default input, press Enter. After going through the initial setup menu, the security appliance displays the summary of the new configuration before prompting the user to accept or reject it.

**Example 3-4  Initial Setup Menu**

```
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]:
Enable password [use current password]: C1$c0123
Allow password recovery [yes]?
Clock (UTC):
   Year [2009]:
   Month [Jul]: Nov
   Day [21]:
   Time [01:08:57]: 21:27:00
Inside IP address: 192.168.10.1
Inside network mask: 255.255.255.0
Host name: Chicago
Domain name: securemeinc.com
IP address of host running Device Manager: 192.168.10.77
```
The following configuration will be used:
Enable password: cisco123
Allow password recovery: yes
Clock (UTC): 21:27:00 Nov 21 2009
Firewall Mode: Routed
Inside IP address: 192.168.10.1
Inside network mask: 255.255.255.0
Host name: Chicago
Domain name: securemeinc.com
IP address of host running Device Manager: 192.168.10.77

Use this configuration and write to flash? yes
INFO: Security level for "inside" set to 100 by default.
WARNING: http server is not yet enabled to allow ASDM access.
Cryptochecksum: e15ea3e4 a499e6cf e84f5b82 1994bde0

1809 bytes copied in 3.490 secs (621 bytes/sec)
Type help or '?' for a list of available commands.
Chicago>

Table 3-2 lists all the parameters that can be configured in the initial setup menu. It also provides a brief description of each parameter, along with the default and configured values.

You can define the initial parameters and features by using either the CLI commands or the ASDM. They are discussed throughout this chapter. The next section discusses how to configure a device name from the ASDM.

Tip You can rerun the interactive setup process by using the setup command in configuration mode.

Initial Setup of ASDM

Before you can access the ASDM graphical console, you must install the ASDM software image on the local flash of the security appliance. The ASDM console can manage a local security appliance only. Therefore, if you need to manage multiple security appliances, the ASDM software must be installed on all the Cisco ASAs. However, a single workstation can launch multiple instances of ASDM clients to manage the different appliances. Optionally, you can leverage Cisco Security Manager (CSM) to configure multiple appliances simultaneously.
### Table 3-2  Initial Setup Parameters and Their Values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
<th>Configured Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable password</td>
<td>Specifies the enable password</td>
<td>None</td>
<td>C1$c0123</td>
</tr>
<tr>
<td>Firewall mode</td>
<td>Sets up the security appliance as a Layer 2 (Transparent) or Layer 3 (Routed) firewall</td>
<td>Routed</td>
<td>Routed</td>
</tr>
<tr>
<td>Inside IP address</td>
<td>Specifies the IP address on the inside interface</td>
<td>None</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>Inside subnet mask</td>
<td>Specifies the subnet mask on the inside interface</td>
<td>None</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Host name</td>
<td>Sets the hostname on the device</td>
<td>ciscoasa</td>
<td>Chicago</td>
</tr>
<tr>
<td>Domain name</td>
<td>Sets the domain name on the device</td>
<td>None</td>
<td>securemeinc.com</td>
</tr>
<tr>
<td>IP address of host running Device Manager</td>
<td>Specifies the IP address of the host machine responsible for managing the Cisco ASA</td>
<td>None</td>
<td>192.168.10.77</td>
</tr>
<tr>
<td>Clock</td>
<td>Sets up the current time on the Cisco ASA</td>
<td>varies</td>
<td>9:27 PM November 21(^{st}) 2009</td>
</tr>
<tr>
<td>Save configuration</td>
<td>Prompts the user if configuration needs to be saved</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow password recovery</td>
<td>Prompts the user if password recovery is allowed</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note**  This book focuses on setting up Cisco ASA through ASDM and the CLI. Configuring ASA through CSM is beyond the scope of this book.

**Uploading ASDM**

You can use the dir command to determine whether the ASDM software is installed. If the security appliance does not have the ASDM software, your first step is to upload the image from an external file server, using the one of the supported protocols. The appliance needs to be set up for basic configuration, such as the interface names, security levels, IP addresses, and proper routes, discussed later in this chapter. After setting up basic information, use the copy command to transfer the image file, as shown in Example 3-5, where an ASDM file, named asdm-621.bin, is being copied from a TFTP server located at...
192.168.10.10. Verify the content of the local flash after the file is successfully uploaded. Copying images is discussed later in this chapter.

**Example 3-5  Uploading the ASDM Image to the Local Flash**

Chicago# copy tftp flash
Address or name of remote host []? 192.168.10.10
Source filename []? asdm-621.bin
Destination filename [asdm-621.bin]? asdm-621.bin

Accessing tftp://192.168.10.10/asdm-621.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Output omitted for brevity.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/asdm-621.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Output omitted for brevity.
6889764 bytes copied in 161.420 secs (36500 bytes/sec)
Chicago# dir
Directory of disk0: /
1260   -rw- 14524416 16:47:34 May 13 2009  asa821-k8.bin
2511   -rw- 6889764 17:38:14 May 13 2009  asdm-621.bin

62881792 bytes total (46723072 bytes free)

Setting Up the Appliance

When the ASDM file is accessed, the Cisco ASA loads the first ASDM image that it finds from the local flash. If multiple ASDM images exist in the flash, use the `asdm image` command and specify the location of the ASDM image you want to load. This ensures that the appliance always loads the specified image when ASDM is launched. In Example 3-6, the appliance is set up to use `asdm-621.bin` as the ASDM image file.

**Example 3-6  Specifying the ASDM Location**

Chicago(config)# asdm image disk0:/asdm-621.bin

The security appliance uses the Secure Socket Layer (SSL) protocol to communicate with the client. Consequently, the security appliance acts as a web server to process the requests from the clients. You must enable the web server on the appliance by using the `http server enable` command.

The security appliance discards the incoming requests until the ASDM client’s IP address is in the trusted network to access the HTTP engine. In Example 3-7, the administrator enables the HTTP engine and sets up the appliance to trust the 192.168.10.0/24 network connected toward the inside interface.
Example 3-7  Enabling the HTTP Server

<table>
<thead>
<tr>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chicago(config)# http server enable</td>
<td></td>
</tr>
<tr>
<td>Chicago(config)# http 192.168.10.0 255.255.255.0 inside</td>
<td></td>
</tr>
</tbody>
</table>

Note The SSL VPN implementation on the appliance also requires you to run the HTTP server on the appliance. Starting from version 8.0, you can set up the security appliance to terminate both the SSL VPN as well as the ASDM sessions on the same interface, using the default port of 443. Use https://<ASAipaddress>/admin to access the GUI for admin and management purposes. This is discussed in Chapter 19.

Accessing ASDM

ASDM’s interface can be accessed from any workstation whose IP address is in the trusted network list. Before you establish the secure connection to the appliance, verify that IP connectivity exists between the workstation and the Cisco ASA.

To establish an SSL connection, launch a browser and point the URL to the appliance’s IP address. In Figure 3-5, the administrator accesses ASDM by entering https://192.168.10.1/admin as the URL. The URL is redirected to https://192.168.10.1/admin/public/index.html.

![Figure 3-5 Accessing the ASDM URL](image-url)
The new security appliance presents its self-signed certificate to the workstation so that a secure connection can be established. If the certificate is accepted, the security appliance prompts the user to present authentication credentials. If the ASDM authentication or enable password is not set up, there is no default username or password. If enable password is defined, there is no default username and you must use enable password as the login password. If user authentication is enabled on the security appliance through use of the `aaa authentication http console` command, then those login credentials must be provided. After a successful user authentication, the appliance presents two ways to launch ASDM:

- **Run ASDM as Java web start application**—The security appliance launches ASDM in the client's browser as a Java applet. This option is not feasible if a firewall that filters out Java applets exists between the client and the security appliance.

- **Run ASDM as a local application**—The security appliance offers a setup utility called `asdm-launcher.msi`, which can be saved to the workstation's local hard drive.

When the ASDM application is launched, it prompts for the IP address of the security appliance to which you are trying to connect, as well as the user authentication credentials. Figure 3-6 illustrates this, where an SSL connection is being made to an appliance located at 192.168.10.1. If you have an enable password configured, specify it under Password and leave the Username blank to log in to ASDM.

![Figure 3-6](image-url)
Note If you are running version 8.2(1) on the security appliance, make sure that you use version 6.2(1) of ASDM. For more information about ASDM, consult http://www.cisco.com/go/asdm.

If the user authentication is successful, ASDM checks the current version of the installer application and downloads a new copy if necessary. It loads the current configuration from the security appliance and displays it in the GUI, as shown in Figure 3-7.

ASDM divides the initial screen, also known as the Home screen, into the following six sections:

- **Device Information**—Displays the hardware and software information of the security appliance, such as the current version of operating system and the device type. If
the License tab is selected, ASDM shows the features that are enabled on the security appliance.

- **VPN Sessions**—Displays the number of active IPSec, clientless, and AnyConnect SSL VPN tunnels
- **System Resources Status**—Provides the current status of CPU and memory usage on the appliance.
- **Interface Status**—Displays the interface name and the assigned IP address. It also shows the link information of the currently configured interfaces and the rate of traffic passing through them.
- **Traffic Status**—Provides information about the number of active TCP and UDP connections and the traffic rate passing through the outside interface.
- **Latest ASDM Syslog Messages**—Shows the latest ASDM syslog messages that are generated by the security appliance. Syslogging is disabled by default and needs to be enabled for log monitoring. When enabled, the security appliance sends the messages to the ASDM client. This is discussed later in the chapter, in the “System Logging” section.

The statistics on the Home screen are refreshed every 10 seconds and show the information for the last 5 minutes.

ASDM shows three additional tabs on the home screen. They include

- **Firewall Dashboard Tab**—The Firewall Dashboard tab presents statistical information about the traffic passing through your security appliance. This includes the number of connections, NAT translations, dropped packets, attacks, and top usage statistics.
- **Content Security Tab**—The Content Security tab displays information about the Content Security and Control (CSC) SSM. This pane appears only if a CSC SSM is installed in the adaptive security appliance.
- **IPS Tab**—The Intrusion Prevention System tab displays information about the IPS module, if present.

**Functional Screens of ASDM**

In addition to the Home screen, the ASDM interface comes with the following two functional screens:

- Configuration screen
- Monitoring screen

**Configuration Screen**

The Configuration screen is useful when the new or existing configuration needs to be modified. On the left side, it contains five to six features icons, depending on the hardware setup of the appliance, as shown in Figure 3-8.
The Feature icons of the Configuration screen are as follows:

- **Device Setup**—Configures interfaces and sub-interfaces on the security appliance. This panel is discussed in the section “Configuring an Interface,” later in the chapter.

- **Firewall**—Helpful in creating security policies to filter and to translate packets traversing through the appliance. Also enables you to define Failover, QoS, AAA, certificates, and many other firewall-related features.

- **Remote Access VPN**—Sets up the remote access VPN connections such as IPSec, L2TP over IPSec, Clientless SSL VPN, and AnyConnect tunnels.

- **Site-to-site VPN**—Sets up the site-to-site VPN tunnels.

- **IPS**—Sets up policies for the SSM card to monitor and drop unauthorized packets. This icon is not visible if an SSM card is not present.

- **Device Management**—Here, the basic device features can be set up. Most of these features are discussed later in this chapter. Helpful in setting up the basic software features, such as system logging and failover.

**Figure 3-8  Configuration Screen**
Monitoring Screen

The Monitoring screen displays statistics about the hardware and software features of the security appliance. ASDM provides real-time graphs to monitor the appliance’s health and status. Figure 3-9 shows the initial Monitoring screen.

```
Figure 3-9  Monitoring Screen
```

Similar to the Configuration screen, the Monitoring screen also displays five or six icons, depending on whether or not you have the SSM module installed.

The Features icons of the Monitoring screen are described below:

- **Interfaces**—Monitors interfaces and sub-interfaces by maintaining ARP, DHCP, and dynamic ACLs tables. It also provides a graphical representation of interface utilization and packet throughput.

- **VPN**—Monitors the active VPN connections on the security appliance. It provides graphs and statistical analysis of the site-to-site, IPSec, and SSL VPN–based remote-access tunnels.

- **IPS**—Provides statistical information for the packets going through the IPS engine. This icon is not present if the IPS module is not installed.
Chapter 3: Initial Setup and System Maintenance

Routing—Displays the current routing table and provides information on EIGRP and OSPF neighbors.

Properties—Monitors active administrative sessions such as Telnet, SSH, and ASDM. It also provides graphical information about CPU, memory, and blocks utilization. Provides graphical information about the active translations and UDP/TCP connections. It provides graphical information of the IP audit, WCCP, CRL, and DNS Cache features.

Logging—Displays log messages as live events. It also shows log messages from the buffer space.

Trend Micro Content Security—ASDM enables you to monitor the CSC SSM statistics, as well as CSC SSM-related features such as types of threats detected by the module, live event logs for real-time monitoring, and resource utilization graphs.

Note If you use ASDM as the primary mode of configuring a security appliance, it is highly recommended that you enable the Preview Command Before Sending Them to the Device option in ASDM. This way, before the commands are pushed to the ASA, ASDM shows them to you for verification. You can enable this feature on ASDM under Tools > Preferences and selecting Preview commands before sending them to the device.

Device Setup

After you have connectivity to the security appliance, either via CLI or ASDM, you are ready to start configuring the device. This section guides you to configure the security appliance for basic setup.

Setting Up Device Name and Passwords

The default device name—also known as the hostname—of a security appliance is ciscoasa. It is highly recommended that you set a unique device name to identify the security appliance on the network. Additionally, networking devices usually belong to a network domain. A domain name appends the unqualified hostnames with the configured domain name. For example, if the security appliance tries to reach a host, secweb, by its hostname and the configured domain name on the security appliance is securemeinc.com, then the fully qualified domain name (FQDN) will be secweb.securemeinc.com.

In a new security appliance, you can configure the Telnet and enable password. The Telnet password is used to authenticate remote sessions either via the Telnet or SSH protocol, discussed later in this chapter. By default, the Telnet password is cisco. For the SSH sessions, the default username is pix. The enable password, on the other hand, gives you access to the privileged exec mode if you are on the user mode. The enable password is also used for ASDM user authentication. There is no enable password by default.
Note If you have user authentication configured for Telnet and/or SSH access, the security appliance does not use the Telnet/enable passwords for those sessions.

To configure the hostname, domain name, and the Telnet/enable passwords via ASDM, navigate to Configuration > Device Setup > Device Name/Password and specify the new settings. As shown in Figure 3-10, the hostname is Chicago and the domain name is securemeinc.com. If you want to configure a new Telnet and/or enable password, select the appropriate change the Telnet and/or enable password option and specify the current and the new passwords. In Figure 3-10, both passwords are set to C1$c0123 (masked).

![Figure 3-10 Configuring Hostname, Domain Name, and Local Passwords](image)

If you prefer to use the CLI, Example 3-8 shows the identical configuration of Figure 3-10. The hostname is changed using the hostname command, the domain name is changed using the domain-name command, and the Telnet and enable passwords are changed using the passwd and enable password commands, respectively.

Example 3-8 Setting Up the Hostname, Domain Name, and Passwords

ciscoasa# configure terminal
ciscoasa(config)# hostname Chicago
Chicago(config)# domain-name securemeinc.com
Chicago(config)# passwd C1$c0123
Chicago(config)# enable password C1$c0123
SYMBOLS

? (question mark), displaying command help in CIPS CLI, 626

AAA (authentication, authorization, accounting)
accounting, 311-313, 340
  RADIUS, 341
  TACACS+, 343
authentication, 311-312
  administrative sessions, 325-336
  ASDM connections, 329
  AuthenticationApp (CIPS), 623
  authentication servers, 318-325
client authentication, 822, 846
  EIGRP, 285, 300
firewall sessions, 330-336
HTTP Form protocol, 318
Individual User Authentication, IPSec
remote-access VPN, 841
interactive client authentication, IPSec remote-access VPN, 840
Kerberos and Active Directory, 318
LDAP, 318
OSPF, 262-267, 279
RADIUS, 314
RIP, 244, 251
SDI, 316-317
serial console connections, 329
SSH connections, 327-328
SSO authentication, 318
TACACS+, 316
telnet connections, 325, 327
troubleshooting administrative connections, 344-347
user authentication, 810-812, 822, 847, 943-946, 1038-1040, 1061
Windows NT, 317
authorization, 311-313, 336-337
command authorization, 338-339
downloadable ACL, 339
TACACS+, 338
DAP configurations, 1007-1009
abbreviating commands, 54
ABR (Area Border Routers), 252
absolute function (time-based ACL), 168
access policies (ASDM), DAP configurations, 1011
Access Method tab, 1016-1017
Action tab, 1012
Bookmarks tab, 1016
Functions tab, 1014
Network ACL tab, 1012
Port Forwarding Lists tab, 1015
Web-Type ACL tab, 1013
accounting, 311-313, 340
RADIUS, 341
TACACS+, 343
ACE (access control entries), 142-143
IPv6 ACL, 158
object grouping, 159
ACL, 164-166
ICMP-type groups, 160
network-based groups, 160
protocol-based groups, 160
service-based groups, 160
syntax/description of, 148-149
thru-traffic filtering via
ASDM, 152-154
CLI, 147, 150
ACL (access control lists)
downloadable ACL, 170-172, 339
encryption ACL, 747
EtherType ACL, 145, 497
extended ACL, 145, 151
configuring for transparent firewalls, 488
SMTF deployment, 497
feature comparison table, 146
ICMP filtering, 172
interface ACL, configuring for transparent firewalls, 487-489
IPv6 ACL, 145, 157-158
monitoring, 193-197
NAT integration, 223-224
object grouping, 159, 164-166
configuring object types, 160-162
ICMP-type groups, 160
network-based groups, 160
protocol-based groups, 160
service-based groups, 160
packet filtering, 2-3, 142-152
QoS packet classification, 586
standard ACL, 144, 166
time-based ACL, 167-170
traffic filtering, inbound traffic, 185-189
web-type ACL, 146, 970-973
Action attribute (ASDM), 153, 156, 220
action rules, QoS configuration via ASDM
traffic policing, 594
traffic prioritization, 593
traffic shaping, 595
Action tab (ASDM), DAP configurations, 1012
active appliances (failover), 521
Active Directory, Kerberos authentication, 318
Active/Active failovers, 528
asymmetric routing, 529-531, 547
configuring, 540
assigning failover group memberships, 545-546
assigning failover interface IP addresses, 542
assigning interface IP addresses, 546
designating primary appliances, 542
enabling failover globally, 548
enabling stateful failover, 542-543
secondary appliance failovers, 548
selecting failover links, 541
setting failover keys, 542
setting up asymmetric routing, 547
setting up failover groups, 543-544
failover MAC addresses, specifying, 552-553
multiple security context deployments
ASDM configurations, 564-566
CLI configurations, 566-568
Active/Standby failovers, 527-528
configuring
assigning failover IP addresses, 535-537
designating primary appliances, 538
enabling failover globally, 539
enabling stateful failover (optional), 538-539
secondary appliance failovers, 540
selecting failover links, 534-535
setting failover keys (optional), 537
failover MAC addresses, specifying, 552-553
single mode deployments
ASDM configurations, 561-562
CLI configurations, 562-564
ActiveX
filtering, 173-175
SSL VPN support, 930
AD (anomaly detection), configuring for AIP-SSM, 666-669
address pools, ASDM configurations
IPSec remote-access VPN, 823
L2TP over IPSec remote-access VPN, 847
address translation, 199
bypassing
identity NAT, 218
NAT exemption, 219-221
configuring, 206-216
interface security levels, 203
ISN randomization, 204
monitoring, 229-230
NAT
ACL integration, 223-224
bidirectional NAT, 201
DNS doctoring, 225-228
dynamic NAT, 209-211
exemptions, 219-221
identity NAT, 218
inside NAT, 200, 207-208
order of operation, 222
policy NAT, 216
static NAT, 207
packet flow sequences, 204
PAT, 202
dynamic PAT, 214-215
policy PAT, 216
static PAT, 212-214
TCP interception, 205-206
admin context (security contexts), 418-419
configuring, 435-436
ASDM configuration using non-shared interfaces, 446-447
ASDM configuration using shared interfaces, 458
MMTF deployments, 505-506
administrative connections, troubleshooting, 344-347
administrative privileges, SSL VPN, 931, 1034
administrative sessions
ASDM connections, 330
authentication
ASDM connections, 329
serial console connections, 329
SSH connections, 327-328
Telnet connections, 325-327
SSH, 328
administrator accounts (AIP-SSM), 632
administrator black list data, configuring for Cisco ASA Botnet Traffic Filter feature, 670-672
Advanced Endpoint Assessment (Host Scan), 1000
AntiSpyware Host Scan, 1003
Antivirus Host Scan, 1002
Firewall Host Scan, 1003
AES (Advanced Encryption Standard), 737
AIP-SSM (Advanced Inspection and Prevention Security Services Module), 615
AD, configuring, 666-669
AIP-SSM-10, 41-43
AIP-SSM-20, 41-43
AIP-SSM-40, 41-43
backup configuration files, creating, 647-648
blocking, configuring, 659-662
CIPS CLI
initializing from, 626, 629-631
logging into AIP-SSM from, 625-626
CLI statistics, displaying, 684-687
configuration information, displaying, 645-646
CS-MARS
adding in, 682
tuning with, 683
CSA integration, 662-666
events
clearing, 650
displaying, 648-649
IP Logging feature
automatic logging, 657-658
configuring, 656
manual logging, 658-659
IPS tuning, 677-681
management interface port, 616-617
trusted hosts, adding, 636-637
upgrading
one-time upgrades, 638-639
scheduled upgrades, 639, 642-643
user accounts
adding/deleting, 633-635
administrator account, 632
operator account, 632
passwords, changing, 635-636
service account, 633
viewer account, 633
Alarm Channel Module, 622
allocate interfaces (security contexts), user context, 433
Analysis Engine Configuration Module, 622
anomaly-based analysis
  IDS, 11-12
  NetFlow, 12
profile-based detection, 11
protocol-based detection, 11
Anti-spam Content Scanning (CSC SSM), 704-706
Anti-spam Email Reputation (CSC SSM), 706-708
AntiSpyware Host Scan, 1003
Antivirus Host Scan, 1002
AnyConnect Essentials licenses, 928, 1028-1030
AnyConnect Mobile licenses, 928, 1029-1030
AnyConnect Premium licenses, 928, 1028-1030
AnyConnect SSL VPN (Secure Sock Layer Virtual Private Network), 1027
  configuring, 1041, 1061
    client configurations, 1055-1059
    CSA, 1042
defining client attributes, 1044-1048
  DNS assignments, 1052
  DTLS configurations, 1053-1054
  keeping SSL VPN client installations, 1053
  loading AnyConnect packages, 1042-1043
  split tunneling, 1049-1051
  SVC versus AnyConnect SSL VPN, 1040
  traffic filter configurations, 1054
  WINS assignments, 1052
deploying, 1059
  enabling address translation for Internet access, 1062
  registry checks, 1061
  user authentication, 1061
monitoring, 1063
Standalone mode, 1042
troubleshooting
  connectivity issues, 1064-1065
  SSL negotiations, 1063
  VPN client versus, 1028
  Web-enabled mode, 1041
application inspection, 350
class-maps, 352
  CTIQBE, 356-358
  DCERPC, 358
  DNS, 359-363
  enabling, 351-353
  ESMTP, 363-366
  FTP, 367-369
  GTP, 369, 373-375
  H.323, 380-382
  HTTP, 390-392
  content-length command, 394
  content-type-verification command, 394
  max-header-length command, 395
  max-uri-length command, 395
  port-misuse command, 396
  request-method command, 396-397
  strict-http command, 393
  transfer-encoding type command, 398
ICMP, 399
ILS protocol, 399-400
IM, 400-402
IPSec pass-through, 403
MGCP, 404-405
NetBIOS, 406
policy-maps, 352
PPTP, 406
RSH, 407
RTSP, 408
selecting inspection, 353-356
service-policies, 352-356
SIP, 408-410
Skinny (SCCP), 410-411
SNMP, 411-412
SQL*Net, 412
Sun RPC protocol, 407
TFTP, 412
UC advanced support
   Mobility Proxy, 389
   phone proxy, 383-388
   Presence Federation Proxy, 390
   TLS proxy, 388-389
WAAS, 413
XDMCP, 413
application proxies (proxy servers),
   network firewalls, 3
arguments, displaying in commands, 54
ARP (address resolution protocol)
   gratuitous ARP, 552
   inspection, enabling in transparent
      firewalls, 492-494
   packets, transparent firewalls, 488
   tests (failover interface tests), 524
ASA (Adaptive Security Appliance)
   administrative connections, troubleshooting, 344-347
AIP-SSM module, 41-43
   appliance access
      CLI, 49, 52-54
      establishing console
         connections, 50-52
      GUI via ASDM, 50
Cisco AIP-SSM module, 41-43
Cisco ASA 5500 Series IPS Solution, 8
Cisco ASA 5505 model, 26-29
Cisco ASA 5510 model, 29-33
Cisco ASA 5520 model, 34-35
Cisco ASA 5540 model, 36
Cisco ASA 5550 model, 36-37
Cisco ASA 5580-20 model, 38-40
Cisco ASA 5580-40 model, 38-42
Cisco ASA Botnet Traffic Filter feature
   configuring, 670
   DNS snooping, 672
   dynamic database, 670-672
   traffic classification, 672-673
commands
   abbreviating, 54
   completing partial command, 54
   displaying description of, 54
   displaying supported arguments/options, 54
   displaying syntax of, 54
configuring, remote-access IPSec
   VPN clients, 914-916
CSC SSM module, 46-47
device setup
   device names/passwords, 67-68
   DHCP services, 76-77
   interface configuration, 69-76
Gigabit Ethernet modules
   Cisco ASA 4GE-SSM, 44
Cisco ASA 5580 expansion cards, 45

initial setup

ASDM setups, 58-64
CLI setups, 57-58

license keys, 54-56
ROMMON mode, 54
image recovery, 105
password recovery process, 106, 109-111

software installation, image upgrades via ASA CLI, 102-104

ASDM (Active Security Device Manager)

Action attribute, 153, 156, 220
AIP-SSM, modifying, 631
ASA, 58
accessing ASDM, 61-64
appliance access, 50
appliance setup, 60
uploading ASDM, 59
authentication, 329, 335-336
certificates, installing, 874-883
Configuration screen, 64-65
certificates, authenticating, 330
CSC SSM monitoring, 715-717
DAP configurations, 1011

Access Method tab, 1016-1017
Action tab, 1012
Bookmarks tab, 1016
Functions tab, 1014
Network ACL tab, 1012
Port Forwarding Lists tab, 1015
Web-Type ACL tab, 1013

Description attribute, 153, 156
Destination attribute, 153, 220
Enable Logging attribute, 153, 156

Enable Rule attribute, 153, 156
Ending IP Address attribute, 209
failovers

Active/Active failover deployments in multiple security contexts, 564-566
configuring Failover Wizard, 548-549
single mode Active/Standby failover deployments, 560-562

Home screen

Content Security tab, 64
Device Information section, 63
Firewall Dashboard tab, 64
Interface Status section, 64
IPS tab, 64
Latest ASDM Syslog Messages section, 64
System Resources Status section, 64
Traffic Status section, 64
VPN Sessions section, 64

image upgrades, 101
Interface attribute, 152, 156, 209, 220
IPSec remote-access VPN configuration, 822-823
L2TP over IPSec remote-access VPN configuration, 848
address pools, 847
client authentication, 846
client-pushed attributes, 847
IKE policies, 847
remote access clients, 846
selecting tunnel type, 846
user authentication, 847
Local CA
configuring, 896-898
enrolling users, 901-904
logging, 119
Logging Interval attribute, 154-156
MMTF deployments (security contexts)
   admin context, 505-506
   system execution space, 504-505
   user context, 507-510
Monitoring screen, 66
NAT Exempt Direction attribute, 220
Netmask attribute, 209
Original Interface attribute, 207
Original Port attribute, 213
Original Source attribute, 207
packet filtering, 152-154
Pool ID attribute, 209
Preview Commands Before Sending Them to the Device option, 67
Protocol attribute, 213
QoS
configuring, 589-595
deployments, 602-604, 607-608
remote-access VPN
   IPSec hairpinning, 856-858
   load balancing, 851-852
Service attribute, 153, 156
site-to-site IPSec VPN deployments, fully meshed topologies with RRI, 775-783
SMTF deployments, 498-500
Source attribute, 153, 156, 220
Source Service attribute, 153, 156
Starting IP Address attribute, 209
Syslog, enabling, 115
Time Range attribute, 154-156
Traffic Direction attribute, 153
traffic filtering
   enabling content filtering via Websense, 190-192
   filtering inbound traffic via ACL, 186-188
Translated Interface attribute, 207
Translated Port attribute, 213
Translated Use IP Address attribute, 207
traded hosts, adding to AIP-SSM, 636-637
virtual firewall deployments
   non-shared interfaces, 445-450
   shared interfaces, 456-462
asymmetric routing, Active/Active failovers, 529-531, 547
Attack Response Controller (CIPS), 622
authentication, 311-312
administrative connections, troubleshooting, 344-347
administrative sessions
   ASDM connections, 329
   firewall sessions, 330-336
   serial console connections, 329
   SSH connections, 327-328
   Telnet connections, 325-327
authentication servers, defining, 318-325
AuthenticationApp (CIPS), 623
client authentication
   ASDM configurations, 822, 846
   IPSec remote-access VPN, 822
   L2TP over IPSec remote-access VPN, 846
EIGRP, 285, 300
HTTP Form protocol, 318
Individual User Authentication, IPSec remote-access VPN, 841
interactive client authentication, IPSec remote-access VPN, 840
Kerberos, Active Directory, 318
LDAP, 318
OSPF, 262-267, 279
RADIUS, 314
RIP, 244, 251
SDI, 316-317
SSO authentication, 318
TACACS+, 316
user authentication
  AnyConnect SSL VPN, 1061
  ASDM configurations, 822
  IPSec remote-access VPN, 810-812, 822
  L2TP over IPSec remote-access VPN, 847
  SSL VPN configurations, 943-946, 1038-1040
Windows NT, 317
authorization, 311-313, 336-337
  command authorization, 338-339
downloadable ACL, 339
  TACACS+, 338
automatic logging, configuring on AIP-SSM, 657-658
AYT (Are you there) messages, 837

backups configuration files, creating for
  AIP-SSM, 647-648
  CSC SSM, 724-725
banner area (SSL VPN logon page), customizing, 951
base license for CSC SSM, installing, 690
Basic Host Scan, 999-1000
bidirectional NAT (Network Address Translation), 201
blocking configuring on AIP-SSM, 659-662
bookmarks, SSL VPN configuration, 965
  bookmark lists, applying to group policies, 969
downloadable ACL, 339
  file servers, 967-968
  SSO servers, 969
  websites, 966-967
Bookmarks tab (ASDM), DAP configurations, 1016
Botnet Traffic Filter feature
  configuring, 670
  DNS snooping, 672
dynamic databases, 670-672
  traffic classification, 672-673
BPDU (bridge protocol data units), transparent firewalls, 488
broadcast ping tests (failover interface tests), 524
browsers
  CSD supported browsers, 983-984
  SSL VPN support, 930, 1032-1034
buffer overflows, memory, 11
buffered logging, 119-121

CA (certificate authority), 871-872.
See also certificates
certificates
  manually importing, 932-933
  SSL VPN configurations, 931-936, 1035
explained, 871-872
Local CA
  configuring, 896-901
  enrolling users, 901-905

caching
  Cache Cleaner, 982, 996-997
  URL server responses, 184

CDP (Cisco Discovery Protocol)
  packets, transparent firewalls, 487
certificates (digital), 870-871. See also CA (certificate authority)
  chain of trust, 871
  CRL, 873
  installing, 883
    ASDM, 874-882
    CLI, 884-896
  IPSec site-to-site tunnels, configuring, 906-910
  manually importing, 932-933
  remote-access IPSec VPN clients, accessing, 910-916
  revoking, 873
  SSL VPN configurations, 931, 1035
    applying ID certificates to SSL VPN connections, 936
    manually importing CA certificates, 932-933
    manually importing ID certificates, 935-936
    requesting certificates, 933-934

chain command, 908

CIFS (Common Internet File System), troubleshooting clientless SSL VPN, 1024-1025

CIPS
  AD, configuring for AIP-SSM, 666-669
  Attack Response Controller, 622
  Authentication App, 623
  cipsWebserver, 623

CLI
  AIP-SSM, initializing, 626-631
  AIP-SSM, logging into, 625-626
  command help, displaying, 626
  configuration command mode, 626
  CtrlTransSource, 625
  EventStore, 624
  Logger, 624
  MainApp, 620-621
  SDEE, 619
  SensorApp, 621-622
  service packs, applying, 637-638
  signatures, customizing, 653-656
  software version, displaying, 643-644

Cisco ASA (Adaptive Security Appliance)
  administrative connections, troubleshooting, 344-347
  AIP-SSM module, 41-43
  appliance access
    CLI, 49, 52-54
    establishing console connections, 50-52
    GUI via ASDM, 50
  Cisco AIP-SSM module, 41-43
  Cisco ASA 5500 Series IPS Solution, 8
  Cisco ASA 5505 model, 26-29
  Cisco ASA 5510 model, 29-33
  Cisco ASA 5520 model, 34-35
  Cisco ASA 5540 model, 36
  Cisco ASA 5550 model, 36-37
  Cisco ASA 5580-20 model, 38-40
  Cisco ASA 5580-40 model, 38-42
Cisco ASA Botnet Traffic Filter feature
- configuring, 670
  - DNS snooping, 672
  - dynamic database, 670-672
  - traffic classification, 672-673
commands
- abbreviating, 54
  - completing partial command, 54
  - displaying description of, 54
  - displaying supported arguments/options, 54
  - displaying syntax of, 54
configuring, remote-access IPSec VPN clients, 914-916
CSC SSM module, 46-47
device setup
  - device names/passwords, 67-68
  - DHCP services, 76-77
  - interface configuration, 69-76
Gigabit Ethernet modules
  - Cisco ASA 4GE-SSM, 44
  - Cisco ASA 5580 expansion cards, 45
initial setup
  - ASDM setups, 58-64
  - CLI setups, 57-58
license keys, 54-56
ROMMON mode, 54
  - image recovery, 105
  - password recovery process, 106, 109-111
software installation, image upgrades via ASA CLI, 102-104
Cisco IP Phone Bypass, IPSec remote-access VPN, 842
Cisco remote-access VPN solution, user authentication, 949, 969, 973
Cisco SAFE architecture, 678
Cisco Secure PIX Firewall, cut-through proxy feature, 330-333
authentication
  - timeouts, 335
  - customizing prompts, 335-336
troubleshooting firewall sessions, 347
class maps
  - application inspection, 352
  - QoS configurations, 597-598
clear configure context command, 439
clearing AIP-SSM events, 650
CLI (command-line interface)
  - AIP-SSM, initializing, 626, 629-631
  - ASA
    - appliance access, 49, 52-54
    - image upgrades, 102-104
    - parameters table, 58
    - setup, 57-58
certificates, installing, 883-896
command help, displaying, 626
configuration command mode, 53
failovers
  - Active/Active failover deployments in multiple security contexts, 566-568
  - single mode Active/Standby failover deployments, 562-564
Local CA
  - configuring, 899-901
  - enrolling users, 904-905
management access rules, defining, 155
MMTF deployments, 510-514
Privileged mode, 53
QoS
  configuring, 597-600
  deploying, 605-606, 609-610
remote-access VPN
  IPSec hairpinning, 858-860
  load balancing, 853-855
site-to-site IPSec VPN deployments
  fully meshed topologies with RRI, 784-789
  single site-to-site tunnel configuration via NAT Traversal, 772-775
SMTF deployments, 501-502
Sub-configuration mode, 53
traffic filtering
  filtering inbound traffic via ACL, 189
  thru-traffic filtering, 147-152
  to-the-box-traffic filtering, 155
User mode, 52
virtual firewall deployments
  non-shared interfaces, 451-454
  shared interfaces, 462-466
Client (PAT) mode, Easy VPN, 826
client authentication
IPSec remote-access VPN
  ASDM configurations, 822
  interactive client authentication, 840
L2TP over IPSec remote-access VPN, ASDM configurations, 846
Client U-turns, 832
client-based SSL VPN (Secure Socket Layer Virtual Private Network), 1027
  configuring, 1061
    client configurations, 1055-1059
CSA, 1042
  defining client attributes, 1044-1048
DNS assignments, 1052
DTLS configurations, 1053-1054
keeping SSL VPN client installations, 1053
loading AnyConnect packages, 1042-1043
split tunneling, 1049-1051
SVC versus client-based SSL VPN, 1040
traffic filter configurations, 1054
WINS assignments, 1052
deploying, 1059
  enabling address translation for Internet access, 1062
  registry checks, 1061
  user authentication, 1061
monitoring, 1063
Standalone mode, 1042
troubleshooting
  connectivity issues, 1064-1065
  SSL negotiations, 1063
VPN client versus, 1028
Web-enabled mode, 1041
client-pushed attributes, ASDM configurations
IPSec remote-access VPN, 823
L2TP over IPSec remote-access VPN, 847
client-server plug-ins, clientless SSL VPN configurations, 979
clientless mode (SSL VPN), 924
  configuring, 947-949
    application access, 973-978
bookmarks, 965-969
client-server plug-ins, 979
full customizations, 960-964
logon page, 951-953, 958-962
logout page, 957
port forwarding, 974-976
portal customization, 957-960
portal page, 955-956, 960, 963-964
smart tunnels, 976-978
web-type ACL, 970-973
deployment scenarios, 1017
DAP configuration, 1020
defining clientless connections, 1019-1020
interfaces, enabling on, 949
monitoring, 1021-1023
troubleshooting
CIFS issues, 1024-1025
CSD, 1025
DAP, 1025-1026
SSL negotiations, 1024
website issues, 1024
VPN client versus, 924
clocks (system), 84
automatic adjustments via NTP, 86
clock set command, 920
manual adjustments, 84-85
commands
abbreviating, 54
authorization, 338-339
configure terminal, 626
description of, displaying, 54
partial commands, completing, 54
Preview Commands Before Sending Them to the Device option (ASDM), 67
session, 616
setup, 627-631
show configuration, 645-646
show events, 648-649
show module, 616
show statistics, 684-687
show statistics analysis-engine, 684-685
show statistics authentication, 685
show statistics event-server, 685
show statistics event-store, 686
show statistics host, 686-687
show statistics logger, 687
show version, 643-644
supported arguments/options, displaying, 54
syntax, displaying, 54
configuration command mode (CIPS CLI), 626
configuration files, backing up
AIP-SSM, 647-648
CSC SSM, 724-725
configuring
AIP-SSM
AD, 666-669
blocking, 659-662
CSA integration, 662-666
IP Logging feature, 656-659
Cisco ASA Botnet Traffic Filter feature
DNS snooping, 672
dynamic database, 670-672
traffic classification, 672-673
configuration management
removing device configuration, 93-94
running configurations, 88-91, 94
startup configurations, 92-94
Configuration mode (CLI), 53
Configuration screen (ASDM), 64-65
configuration URL, specifying in security contexts, 434-435
configure terminal command, 53, 626
CSC SSM
  FTP file blocking, 712-713
  FTP scanning, 709-712
  initial setup, 690-694
  mail-based features, 701-709
  management interface, 690
  syslog, 718-719
  web-based features, 694-701
security contexts, 429
  transparent firewalls, 484
connection profiles, site-to-site VPN, 741-743, 753-755
console logging, 118
console ports, establishing ASA appliance connections, 50-52
content area (SSL VPN portal page), customizing, 956
content filtering, 173
  ActiveX filtering, 173-175
  configuring, 174-175
  Java filtering, 174-175
  monitoring, 198
  SMTP Content Filtering (CSC SSM), 708-709
  Websense, enabling filtering via, 190-192
Content Security tab (ASDM Home screen), 64
content-length command, HTTP inspection, 394
content-type-verification command, HTTP inspection, 394
copy and paste method, installing certificates from, 877
copyright area (SSL VPN logon page), customizing, 953
CoS (class of service). See traffic prioritization
CPP (Centralized Protection Policies), 838
CPU (central processing units)
  monitoring, 133-134
  troubleshooting, 139
CRL (certificate revocation list), 873
  configuring options, 893-896
  retrieval, troubleshooting PKI, 921
crypto ca authenticate command, 887, 890
crypto ca crl request command, 895
crypto ca enroll command, 887-888, 891
crypto ca import command, 892
crypto ca server command, 899
crypto ca server user-db add command, 904
crypto ca server user-db allow command, 904
crypto ca server user-db email-otp username command, 905
crypto ca trustpoint command, 884
crypto key generate rsa command, 883
crypto key zeroize rsa command, 884
crypto maps
  IPSec remote-access VPN, 816-817
  site-to-site IPSec VPN, 745-749
CS-MARS (Cisco Secure Monitoring and Response System)
AIP-SSM, 682-683
NetFlow, 12
supported devices and technologies, 681-682
CSA (Cisco Security Agent), 8
AnyConnect SSL VPN clients, 1042
configuring, 662-666
CSC SSM (Content Security and Control Security Services Module), 46-47
backup configuration files, creating, 724-725
base licenses, installing, 690
FTP
   file blocking, 712-713
   scanning, 709-712
initial configuration, 690-694
installation issues, troubleshooting, 722
live security event messages, monitoring, 717
mail-based features
   POP3 support, configuring, 709
SMTP Anti-spam Content Scanning, 704-706
SMTP Anti-spam Email Reputation, 706-708
SMTP Content Filtering, 708-709
SMTP scanning, 701-704
management interfaces, configuring, 690
monitoring, 715
password recovery, 722-724
re-imaging, 719-721
software upgrades, 726
tsmlg, configuring, 718-719
troubleshooting tools, 726
   Gather Logs, 733-734
   Management Port Console Access Settings, 734
   Show System Information, 727-733
web-based features, 694
   file blocking, 697-698
   HTTP scanning, 699-701
   URL blocking, 695-697
CSD (Cisco Secure Desktop), 980-981
AnyConnect SSL VPN registry checks, 1061
architecture, 984
Cache Cleaner, 982, 996-997
configuring
   defining prelogin sequences, 987-998
   loading CSD packages, 985
Host Scan, 998
   Advanced Endpoint Assessment, 1000-1003
   Basic Host Scan, 999-1000
   Endpoint Assessment, 999, 1002
requirements
   supported browsers, 983-984
   supported operating systems, 983
   user privileges, 983
Secure Desktop (Secure Session), 982, 992-995, 998
Secure Desktop Manager, 982
troubleshooting, 1025
CTIQBE (Computer Telephony Interface Quick Buffer Encoding Inspection), 356-358
D

DAP (dynamic access policies), 1003
architecture of, 1004-1005
clientless SSL VPN configurations, 1020
configuring, 1006

defining access policies, 1011-1017

selecting AAA attributes, 1007-1009

selecting endpoint attributes, 1009

sequence of events, 1005
troubleshooting, 1025-1026

DAPR (dynamic access policy records), 1005
data-passing interface, configuring
(ASA device setup), 69-73
date/time
mismatches, troubleshooting PKI, 917-920
system clocks

manual adjustments, 85
time zones, 84
time mode (authentication servers), 323

Time Range attribute (ASDM), 154-156
DCERPC (Distributed Computing Environment Remote Procedure Calls), 358
DCS (Direct Call Signaling), 382
DDoS (Dedicated Denial of Service) attacks, 11-12
debugging
debuge crypto ca command, 917
debuge crypto ca messages command, 920
debuge crypto ca transactions command, 920
debuge crypto isakmp 127 command, 917
debuge logs, 719

L2F table entries, transparent firewalls, 516
multicast routing, troubleshooting, 309-310
deep packet inspection, 7
default gateways, setting up in transparent firewalls, 487
defered scanning (CSC SSM), 711
dense mode (PIM-DM), 302
depletion mode (authentication servers), 323
Description attribute (ASDM), 153, 156
desktops, CSD, 980-981

AnyConnect SSL VPN registry checks, 1061
architecture, 984
Cache Cleaner, 982, 996-997
configuring, 985-998
Host Scan, 998-1003
requirements, 983-984
Secure Desktop (Secure Session),
982, 992-995, 998
Secure Desktop Manager, 982
supported browsers, 983-984
supported operating systems, 983
troubleshooting, 1025
user privileges, 983
Destination attribute (ASDM), 153,
220
device configuration, removing,
93-94
Device Information section (ASDM
Home screen), 63
Device Management icon (ASDM
Configuration screen), 65
device setup (ASA)
device names/passwords, 67-68
DHCP services, 76-77
interface configuration
data-passing interface, 69-73
management interface, 75-76
routed mode, 70
subinterface, 73-74
Device Setup icon (ASDM
Configuration screen), 65
device-level failovers, 527
Active/Active failovers, 528, 540
assigning failover group
memberships, 545-546
assigning failover interface IP
addresses, 542
assigning interface IP
addresses, 546
asymmetric routing, 529-531,
547
designating primary
appliances, 542
enabling failover globally, 548
enabling stateful failover,
542-543
multiple security context
deployments, 564-568
secondary appliance failovers,
548
selecting failover links, 541
setting failover keys, 542
setting up asymmetric routing,
547
setting up failover groups,
543-544
specifying failover MAC
addresses, 553-554
Active/Standby failovers, 527-528,
534
assigning failover IP addresses,
535-537
designating primary
appliances, 538
enabling failover globally, 539
enabling stateful failover
(optional), 538-539
secondary appliance failovers,
540
selecting failover links, 534-535
setting failover keys (optional),
537
single mode deployments,
560-564
specifying failover MAC
addresses, 552-553
DHCP (Dynamic Host Configuration
Protocol) services, ASA device
setup (ASA), 76-77
Diffie-Hellman exchanges
IPSec, 17
PFS, 19
digital certificates, 870-871. See also
CA (certificate authority)
chain of trust, 871
CRL, 873
installing, 883
  ASDM, 874-882
  CLI, 884-896
IPSec site-to-site tunnels,
  configuring, 906-910
manually importing, 932-933
remote-access IPSec VPN clients,
  accessing, 910-916
revoking, 873
SSL VPN configurations, 931, 1035
  applying ID certificates to SSL
  VPN connections, 936
  manually importing CA
  certificates, 932-933
  manually importing ID
  certificates, 935-936
  requesting certificates, 933-934
Dijkstra algorithm, 252
disabling
  password recovery process, 109-113
  signatures (IPS), 679-680
displaying
  AIP-SSM configuration information,
    645-646
  AIP-SSM events, 648-649
  CIPS software version, 643-644
  OSPF neighbor information, 274
  statistics for AIP-SSM, 684-687
DIT (Directory Information Trees),
    318
DMZ (demilitarized zones), firewall
  configurations, 6
DNS (Domain Name Servers)
  AnyConnect SSL VPN assignments,
    1052
  application inspection, 359-363
  DNS doctoring, 225-226, 228
  dns name-server ip-address command, 895
  IPSec remote-access VPN, 821
  snooping, configuring for Cisco ASA
  Botnet Traffic Filter feature, 672
domain names, ASA device setup, 67-68
downloadable ACL (access control
lists), 170-172, 339
dropped packets, monitoring, 138-139
DSCP (Differentiated Services Code
Point), IP DSCP field (QoS packet
classification), 583-586
DTLS (Datagram Transport Layer
Security), AnyConnect SSL VPN
configurations, 1053-1054
DUAL (Diffusing Update Algorithm),
    280
dynamic database, configuring for
  Cisco ASA Botnet Traffic Filter
  feature, 670-672
dynamic NAT (Network Address
Translation), global pools
  configuring, 210-211
  defining, 209
  mapping to real addresses, 211
dynamic PAT (Port Address
Translation), 214-215
dynamic routing over VPN, OSPF,
    270-272

E

Easy VPN (Virtual Private Networks)
  Client (PAT) mode, 826
IPSec remote-access VPN

Cisco IP Phone Bypass, 842

hardware-based VPN client configurations, 826-828

Individual User Authentication, 841

interactive client authentication, 840

LEAP Bypass, 842

software-based VPN client configurations, 824

NEM, 826, 842

EIGRP (Enhanced Interior Gateway Routing Protocol)

authentication, 285, 300
controlling default information, 291-292
enabling, 280-284
route filtering, 284
route redistribution, 289-291
route summarization, 287
split horizon, 288
static neighbors, defining, 286-287
troubleshooting

authentication, 300
commands, 292-295
hello intervals, 297-300
hold intervals, 297-300
link failures, 296-297

email

Anti-spam Email Repudiation (CSC SSM), 706-708
logging, 119
servers, defining, 122

Enable Logging attribute (ASDM), 153, 156

Enable Rule attribute (ASDM), 153, 156

encryption

ACL, 747
AES, 737

Ending IP Address attribute (ASDM), 209

dependencies

Endpoint Assessment (Host Scan), 999, 1002
endpoint attributes, DAP configurations, 1009

enrolling

Cisco VPN clients, 911-914
enrollment process, 874
ESMTP (Extended SMTP), application inspection, 363-366
Ethernet, Gigabit Ethernet modules
Cisco ASA 4GE-SSM, 44
Cisco ASA 5580 expansion cards, 45
EtherType ACL (access control lists), 145, 497
event lists, defining (system logging), 116-117
events (AIP-SSM)
clearing, 650
displaying, 648-649
EventStore (CIPS), 624

extended ACL (access control lists), 145, 151

SMTF deployment, 497
transparent firewalls, configuring for, 488

failovers

active appliances, 521
conditions that trigger failover, 523
control links, 522
failovers

device-level failovers

*Active/Active failovers*, 528-531, 540-548, 553-554, 564-568

*Active/Standby failovers*, 527-528, 534-540, 552-553, 560-564

Failover Wizard (ASDM), configuring, 548-549

hardware requirements, 525-526

interface-level failovers

*multiple-mode firewalls*, 551

*redundant interface guidelines*, 531-533

*single-mode firewalls*, 550

interfaces

*monitoring*, 556-557

*policy configuration*, 554

*tests*, 523-524

MAC addresses, specifying

*Active/Active failovers*, 553-554

*Active/Standby failovers*, 552-553

monitoring, 569-572

software requirements, 525-526

standby appliances, 521

stateful failovers, 524-526

*Active/Active failovers*, 542-543

*Active/Standby failovers*, 538-539

stateless failovers, 524

timers, managing, 555

troubleshooting, 572-574

zero-downtime software upgrades, 557-559

false positives, pattern matching, 10

file blocking (CSC SSM), configuring, 697-698

file servers

clientless SSL VPN configurations, 967-968

defining, 968

*FILENAME*, 501

filtering

OSPF Type 3 LSA filtering, 268-270

packet filtering

*ACE*, 142-143, 147-157

*ACL*, 142-152

*traffic filtering*, 147-158, 185-192

PIM neighbors, multicast routing, 307

route filtering

*EIGRP routes*, 284

*RIP routes*, 246-248

traffic filtering

*AnyConnect SSL VPN configurations*, 1054

*deployment scenarios*, 185-192

*IPSec remote-access VPN*, 817-818

*IPv6 ACL setup*, 157-158

*packet filtering*, 147-158, 185-192

*site-to-site IPSec VPN*, 749-750

*thru-traffic filtering*, 147-154

*to-the-box-traffic filtering*, 154-156

firewalls

authentication, 330-333

*customizing prompts*, 335-336

*session authentication*, 332

*timeouts*, 335

Cisco Secure PIX Firewall,
cut-through proxy feature, 330-336, 347
deep packet inspection, 7
developing, 1
DMZ configurations, 6
Firewall Dashboard tab (ASDM Home screen), 64
Firewall Host Scan, configuring, 1003
Firewall icon (ASDM Configuration screen), 65
multiple-mode firewalls
  interface-level redundancy, 551
  single-mode firewalls versus, 419-421
network firewalls
  application proxies (proxy servers), 3
  NAT, 3-5
  packet-filtering, 2-3
personal firewalls, 2, 7
routed firewalls, 471
  enabling, 484
  transparent firewalls versus, 472-474
sessions, troubleshooting, 347
single-mode firewalls
  interface-level redundancy, 550
  multiple-mode firewalls versus, 419-421
stateful inspection firewalls, 6
transparent firewalls, 471
  configuring, 482-496
  MMTF, 477, 496, 502-514
  monitoring, 514-516
  NAT, 479-481
  restrictions within, 479-481
  routed firewalls versus, 472-474
  SMTF, 474-476, 496-502

troubleshooting, 516-519
VPN, 479
virtual firewalls, deploying using
  non-shared interfaces, 443-454
  shared interfaces, 454-466
VPN client firewalls, IPSec remote-access VPN, 836-838

Flash logging, 123
FoIP (Fax over IP), T.38 protocol, 382
fragmentation (packets), site-to-site IPSec VPN, 767-768
FTP (File Transfer Protocol)
  application inspection, 367-369
  file blocking (CSC SSM), 712-713
  filtering, 180-182
  FTP servers, saving security contexts to, 469
  logging, 124
  scanning (CSC SSM), 709-712

full tunnel mode (SSL VPN), 924, 1027
  configuring, 1041, 1061
  client configurations, 1055-1059
  CSA, 1042
  defining client attributes, 1044-1048
  DNS assignments, 1052
  DTLS configurations, 1053-1054
  keeping SSL VPN client installations, 1053
  loading AnyConnect packages, 1042-1043
  split tunneling, 1049-1051
  SVC versus full tunnel SSL VPN, 1040
traffic filter configurations, 1054
   WINS assignments, 1052
deploying, 1059
   enabling address translation
   for Internet access, 1062
registry checks, 1061
user authentication, 1061
monitoring, 1063
Standalone mode, 1042
troubleshooting
   connectivity issues, 1064-1065
   SSL negotiations, 1063
VPN client versus, 1028
Web-enabled mode, 1041
Functions tab (ASDM), DAP
configurations, 1014

G

gatekeepers (H.323), 376
gateways
   H.323 gateways, 376
tunnel default gateways
     IPSec remote-access VPN, 828
     site-to-site IPSec VPN, 759-760
Gather Logs tool (CSC SSM), 733-734
Gigabit Ethernet modules
   Cisco ASA 4GE-SSM, 44
   Cisco ASA 5580 expansion cards, 45
GKRCs (Gatekeeper Routed Control
Signaling), 382
global configuration mode (CIPS 5.x), 626
global pools (dynamic NAT)
   configuring, 210-211
defining, 209
   mapping to real addresses, 211
   global unicast addresses, IPv6
   configuration, 81
GMP stub mode, 301
GPRS (General Packet Radio Service),
   GTP
      application inspection, 374-375
      GTPv0, 369-371
      GTPv1, 372-373
   gratuitous ARP (address resolution
   protocol), 552
GRE (Generic Routing Encapsulation)
   Protocol, VPN, 13
group policies
   applying bookmark lists to (clientless
   SSL VPN configurations), 969
   IPSec remote-access VPN, setting up
group policies, 806
   mapping
      port forwarding lists to (clientless
      SSL VPN configuration), 976
      smart tunnel lists to (SSL VPN
      configurations), 978
   SSL VPN configurations, 937-941,
   1035-1036
GTP (GPRS Tunneling Protocol)
   application inspection, 369, 373-375
   GTPv0, 369-371
   GTPv1, 372-373
GUI (graphical user interface), ASA
   appliance access via ASDM, 50

H

H.323
   application inspection, 380-382
   DCS, 382
gatekeepers, 376
gateways, 376
GKRCS, 382
MCU, 376
protocol suite, 376-377
RAS protocol, 378
RTCP, 377
T.38 protocol, 382
terminals, 376
version compatibility, 378
hairpinning (IPSec)
  IPSec remote-access VPN, 831
L2TP over IPSec remote-access VPN
    ASDM configurations, 856-858
    CLI configurations, 858-860
hello intervals, troubleshooting in EIGRP, 297-300
heuristic scanning, IDS, 11
HIPS (host intrusion prevention systems), 8
hold intervals, troubleshooting in EIGRP, 297-300
Home screen (ASDM)
  Content Security tab, 64
  Device Information section, 63
  Firewall Dashboard tab, 64
  Interface Status section, 64
  IPS tab, 64
  Latest ASDM Syslog Messages section, 64
  System Resources Status section, 64
  Traffic Status section, 64
  VPN Sessions section, 64
hop counts, 240
host emulators, CSD prelogin sequences, 990-991

Host Scan, 998
  Advanced Endpoint Assessment, 1000
    AntiSpyware Host Scan, 1003
    Antivirus Host Scan, 1002
    configuring, 1002-1003
    Firewall Host Scan, 1003
  Basic Host Scan, 999-1000
  Endpoint Assessment, 999, 1002
hostnames, ASA device setup, 67-68
HTTP (Hypertext Transfer Protocol)
  application inspection, 390-392
    content-length command, 394
    content-type-verification command, 394
    max-header-length command, 395
    max-uri-length command, 395
    port-misuse command, 396
    request-method command, 396-397
    strict-http command, 393
    transfer-encoding type command, 398
  filtering, configuring, 180-182
  HTTP Form protocol, 318
  scanning (CSC SSM), 699-701
HTTPS (HTTP over SSL/TLS)
  filtering, configuring, 180-182
  SSL VPN, 21-22
HyperTerminal
  configuring, 50
  connection type, setting, 51
  port specification, setting, 52
ICMP (Internet Control Message Protocol)
filtering, ACL, 172
ICMP-type object groups, 160
inspection, 399
ICSA (International Computer Security Association), 619
ID certificates, manually importing, 935-936
IDCONF (Intrusion Detection Configuration) protocol, 622
identity NAT (Network Address Translation), 218
IDS (intrusion detection systems), 8
anomaly-based analysis, 11-12
DDoS attacks, 11-12
heuristic scanning, 11
pattern matching
  false positives, 10
  signatures, 9
  stateful pattern-matching recognition, 10
protocol analysis, NIDS, 10
IGMP (Internet Group Management Protocol), multicast routing
query timeouts, 304
State Limit feature, 303-304
static group assignments, 302
version of, defining, 304
IKE (Internet Key Exchange) protocol
IPSec, 14, 18
IPSec remote-access VPN, ASDM configurations, 823
L2TP over IPSec remote-access VPN, ASDM configurations, 847
ILS (Internet Locator Service) protocol, inspection, 399-400
IM (Internet Messenger), inspection, 400-402
images
  ROMMON, 54, 105
upgrades
  ASA CLI, 102-104
  ASDM, 101
incoming SMTP scanning (CSC SSM), configuring, 701-704
Individual User Authentication, IPSec remote-access VPN, 841
information area (SSL VPN logon page), customizing, 953
initial Cisco ASA setup, interface configuration, 71
initial CSC SSM configuration, 690-694
initializing AIP-SSM from CIPS CLI, 626, 629-631
inline IPS mode, traffic flow, 617
inside NAT (Network Address Translation), 200, 207-208
inspect dns command, 363
inspection (application), 350
class-maps, 352
CTIQBE, 356-358
DCERPC, 358
DNS, 359-363
enabling, 351-353
ESMTP, 363-366
FTP, 367-369
GTP, 369, 373-375
H.323, 380-382
HTTP, 390-392
  content-length command, 394
content-type-verification command, 394
max-header-length command, 395
max-uri-length command, 395
port-misuse command, 396
request-method command, 396-397
strict-http command, 393
transfer-encoding type command, 398

ICMP, 399
ILS protocol, 399-400
IM, 400-402
IPSec pass-through, 403
MGCP, 404-405
NetBIOS, 406
policy-maps, 352
PPTP, 406
RSH, 407
RTSP, 408
selective inspection, 353-356
service-policies, 352-356
SIP, 408-410
Skinny (SCCP), 410-411
SNMP, 411-412
SQL*Net, 412
Sun RPC protocol, 407
TFTP, 412
UC advanced support
  Mobility Proxy, 389
  phone proxy, 383-388
  Presence Federation Proxy, 390
  TLS proxy, 388-389
WAAS, 413
XDMCP, 413

installing
certificates
  ASDM, 874-883
  CLI, 883-896
CSC SSM
  base licenses, 690
  troublesooting, 722
software, 101
  image recovery, 105
  image upgrades, 101-104
IntelliTrap feature (CSC SSM), 702
interactive client authentication, IPSec
remote-access VPN, 840

interfaces
ACL, transparent firewalls, 487-489
configuring (ASA device setup)
  data-passing interface, 69-70, 72-73
  management interface, 75-76
  routed mode, 70
  subinterface, 73-74
failovers
  multiple-mode firewalls, 551
  policy configuration, 554
  redundant interface guidelines, 531-533
  single-mode firewalls, 550
Interface attribute (ASDM), 152, 156, 209, 220
Interface Status section (ASDM
  Home screen), 64
Interfaces icon (ASDM Monitoring
  screen), 66
security levels, address translation
  and, 203
tests (failover), 523-524
IP addresses
IPSec remote-access VPN assignments, 812-816
transparent firewall configuration, 485

IP DSCP field (QoS packet classification), 583-586

IP flow, QoS packet classification, 587

IP logger statistics, displaying, 687

IP Logging feature (AIP-SSM)
automatic logging, 657-658
configuring, 656
manual logging, 658-659

IP multicast routing
configuring RP, 306
enabling, 302
enabling PIM, 305
filtering PIM neighbors, 307
GMP stub mode, 301

IGMP
defining IGMP version, 304
limiting IGMP states, 303-304
query timeouts, 304
statically assigning IGMP groups, 302
PIM-SM, 302
static multicast routes, 307-308
troubleshooting
debuge commands, 309-310
show commands, 308-309

IP Phone Bypass, IPSec remote-access VPN, 842

IP Precedence field (QoS packet classification), 583

IP routing
EIGRP
authentication, 285, 300

controlling default information, 291-292
defining static neighbors, 286-287
enabling, 280-284
route filtering, 284
route redistribution, 289-291
route summarization, 287
split horizon, 288
troubleshooting, 292-300

multicast routing
configuring RP, 306
defining IGMP version, 304
enabling, 302
enabling PIM, 305
filtering PIM neighbors, 307
GMP stub mode, 301
IGMP query timeouts, 304
limiting IGMP states, 303-304
PIM-SM, 302
static multicast routes, 307-308
statically assigning IGMP groups, 302
troubleshooting, 308-310

OSPF, 252
authentication, 262-267, 279
dynamic routing over VPN, 270-272
enabling, 254-258
neighbor command, 270-271
NSSA, 268
redistribution, 266-267
stub areas, 267
troubleshooting, 273-279
Type 3 LSA filtering, 268-270
virtual links, 259-261, 264-267
VPN tunneling, 272
RIP, 240
  *authentication*, 244, 251
  *configuring*, 241-243
  *redistribution*, 249
  *route filtering*, 246-248
  *troubleshooting*, 250-252

static routing, 231-232
  *displaying routing tables*, 239-240
  *monitoring*, 234-235, 238

**IPS (intrusion prevention systems), 8-9**

**CIPS**
  *Attack Response Controller*, 622
  *AuthenticationApp*, 623
  *cipsWebserver*, 623
  *CtlTransSource*, 625
  *EventStore*, 624
  *Logger*, 624
  *MainApp*, 620-621
  *SensorApp*, 621-622

Cisco ASA 5500 Series IPS Solution, 8

**CSA, 8**

**DDoS attacks, 11-12**

**HIPS, 8**

inline IPS mode, traffic flow, 617

**IPSec (IP Security)**

**Diffie-Hellman exchanges, 17**
monitoring, 860-864
setting up group policies, 806
setting up tunnel groups, 808
software-based VPN client configurations, 824
split tunneling (optional), 818-819
traffic filtering (optional), 817-818
transparent tunneling, 829-831
troubleshooting, 865-867
tunnel default gateways, 828
VPN client firewalls, 836-838
VPN load balancing, 833-835
WINS (optional), 821
site-to-site IPSec VPN, 735
bypassing NAT (optional), 751
Connection Profiles, 753-755
connection types, 764-765
creating ISAKMP policies, 739-740
crypto maps, 745-749
defining IPSec policies, 743-745
enabling ISAKMP, 739
fully meshed topologies with RRI, 775-789
IPSec VPN Wizard, 752-753
keepalives feature (ISAKMP), 766
management access, 760
monitoring, 789-792
NAT Traversal, 758-759
OSPF updates over IPSec, 755-756
packet fragmentation, 767-768
PFS, 761
Phase 1 mode, 764
preconfiguration checklist, 736-737
RRI, 757-758, 775-789
security association lifetimes, 763-764
setting up tunnel groups, 741-743
single site-to-site tunnel configuration via NAT Traversal, 769-775
traffic filtering (optional), 749-750
troubleshooting, 793-798
tunnel default gateways, 759-760
site-to-site tunnels, configuring with certificates, 906-910
Transport mode, 20
Tunnel mode, 20
VPN, 13-20
IPv6 (Internet Protocol version 6), 78
ACL, 145, 157-158
configuring
global unicast addresses, 81
IP address assignment, 80-82
link-local addresses, 82
site-local addresses, 82
headers, 78-80
neighbor reachable time, 83
neighbor solicitation messages, 83
optional parameter setup, 83
router advertisement transmission intervals, 83
ISAKMP (Internet Security Association and Key Management Protocol)
IPSec, 14-16
IPSec remote-access VPN, 802-804
site-to-site IPSec VPN
    creating ISAKMP policies, 739-740
    enabling ISAKMP, 739
    keepalives feature, 766
    troubleshooting, 795-798
isakmp identity auto command, 907
ISN (Initial Sequence Numbers), randomization, 204

J - K

Java filtering, 174-175

keepalives
    AYT messages, 837
    keepalives feature (ISAKMP), site-to-site IPSec VPN, 766
Kerberos
    Active Directory authentication, 318
    user authentication, SSL VPN configurations, 943, 1038
key pairs, generating in CLI, 883-884
keysize command, 899
keysize server command, 899
keystroke loggers, CSD prelogin sequences, 990-991

L

L2F (Layer 2 Forwarding) Protocol
    L2F tables
        aging time, transparent firewalls, 496
        clearing tables associated with outside interfaces, 519
    statif L2F tables, adding entries to transparent firewalls, 492
    transparent firewalls, debugging entries, 516
    VPN, 13
L2TP (Layer 2 Tunneling Protocol)
    L2TP over IPSec remote-access VPN, 843
        ASDM configuration, 846-848, 856-858
        CLI configuration, IPSec hairpinning, 858-860
        IPSec remote-access VPN over, 800
    VPN, 13
Latest ASDM Syslog Messages section (ASDM Home screen), 64
LDAP (Lightweight Directory Access Protocol), 318
LEAP Bypasses, IPSec remote-access VPN, 842
license keys
    changing, 56
    information about, displaying, 54-55
    lifetime ca-certificate command, 899
    link up/down tests (failover interface tests), 523
    link-local addresses, IPv6 configuration, 82
    links
        EIGRP link failures, troubleshooting, 296-297
        virtual links, OSPF, 259-261, 264-267, 279
    live security event messages (CSC SSM), monitoring, 717
    LLQ (low-latency queue). See traffic prioritization
load balancing
- IPSec remote-access VPN, 833-835
- remote-access VPN, 849-855

Local CA (Local Certificate Authority)
configuring via
  - ASDM, 896-898
  - CLI, 899-901
enrolling users via
  - ASDM, 901-904
  - CLI, 904-905

local disks, saving security contexts to, 468

logging
- AIP-SSM, logging into from CIPS
  - CLI, 625-626
- console logging, 118
- debug logs, 719
- Flash logging, 123
- FTP logging, 124
- IP logger statistics, displaying, 687
- IP Logging feature (AIP-SSM)
  - automatic logging, 657-658
  - configuring, 656
  - manual logging, 658-659
- Logger (CIPS), 624
- Logging icon (ASDM Monitoring screen), 67
- Logging Interval attribute (ASDM), 154, 156
- system logging
  - ASDM logging, 119
  - buffered logging, 119-121
  - console logging, 118
  - email logging, 119
  - email servers, 122
  - enabling, 114-115
  - event lists, 116-117
  - logging lists, 120-121
  - storing logs internally/externally, 123-124
  - Syslog server logging, 119-122
  - terminal logging, 119

logon page (SSL VPN), customizing
- banner area, 951
- copyright area, 953
- full customizations, 960-962
- information area, 953
- logon area, 952
- user connection profiles, 958-959

logout page (SSL VPN), customizing, 957

lost passwords, recovering for CSC SSM, 722-724

LSA (link-state advertisements), OSPF
  - Type 3 LSA filtering, 268-270

MAC addresses
- failover MAC addresses, specifying
  - Active/Active failovers, 553-554
  - Active/Standby failovers, 552-553
- packet classification (security contexts), 424

mail-based features (CSC SSM)
- POP3 support, 709
- STMP Anti-spam Content Scanning, 704-706
- STMP Anti-spam Email Reputation, 706-708
- STMP Content Filtering, 708-709
- STMP scanning, 701-704
main root CA (certificate authority), 871
main.log files, accessing, 624
MainApp (CIPS), 620-621
management interfaces
  configuring (ASA device setup), 75-76
  management interface port (AIP-SSM), 616-617
Management Port Console Access Settings tool (CSC SSM), 734
manual logging, configuring on AIP-SSM, 658-659
master blocking sensors, 622
match command, selective application inspection, 353-354
max-header-length command, HTTP inspection, 395
max-uri-length command, HTTP inspection, 395
MCU (multipoint control units), H.323, 376
memory
  buffer overflows, 11
  monitoring, 133-134
message ID tuning (Syslog), 124
MGCP (Media Gateway Control Protocol), inspection, 404-405
MMTF (multimode transparent firewalls), 477, 496
deploying with security contexts, 502-504
  ASDM deployments, 504-510
  CLI deployments, 510-514
  packet flow, 477
Mobility Proxy, UC advanced support, 389
mode-config, 800
monitoring
  AnyConnect SSL VPN, 1063
  clientless SSL VPN, 1021-1023
  CPU, 133-134
  CSC SSM, 715-717
dropped packets, 138-139
  failovers, 569-572
  memory, 133-134
  Monitoring screen (ASDM), 66
  QoS, 611-612
  remote-access VPN, 860-864
  security contexts, 466-467
  site-to-site IPSec VPN, 789-792
SNMP, 133
  system monitoring
    NSEL, 125-128
    SNMP, 128-133
    system logging, 113-124
  transparent firewalls, 514-516
MPF (Modular Policy Framework), deep packet inspection, 7
MPLS (Multiprotocol Label Switching)
  transparent firewalls, 488
VPN, 13
multicast routing (IP)
  configuring RP, 306
  enabling, 302
  enabling PIM, 305
  filtering PIM neighbors, 307
  GMP stub mode, 301
IGMP
  defining IGMP version, 304
  query timeouts, 304
  statically assigning IGMP groups, 302-304
  PIM-SM, 302
  static multicast routes, 307-308
troubleshooting
  debug commands, 309-310
  show commands, 308-309

multiple mode
  firewalls
    interface-level redundancy, 551
  single-mode firewalls versus, 419-421
  packet flow in (security contexts), 424-426

N

N (distinguished names), 318
naming devices, ASA device setup, 67-68
NAS (network access servers), 314
NAT (Network Address Translation), 3
  ACL integration, 223-224
  bidirectional NAT, 201
  DNS doctoring, 225-228
  dynamic NAT
    configuring global pools, 210-211
    defining global pools, 209
    mapping global pools to real addresses, 211
  exemptions, 219-221
  identity NAT, 218
  inside NAT, 200, 207-208
  IPSec remote-access VPN, bypassing in, 818
  NAT Traversal, site-to-site IPSec VPN, 758-759, 769-775
  order of operation, 222
  PAT, 4
  policy NAT, 216
  site-to-site IPSec VPN, bypassing
    NAT, 751
    static NAT, 207
    static translation, 5
    transparent firewalls, 479-481, 491
  NAT Exempt Direction attribute (ASDM), 220
  NAT-T (Network Address Translation-Traversal)
    IPSec remote-access VPN, 829-830
  VPN, 18
  navigation panel (SSL VPN portal page), customizing, 955-956
  neighbor command (OSPF), 270-271
  neighbor reachable time (IPv6), 83
  neighbor solicitation messages (IPv6), 83
  NEM (Network Extension Mode), Easy VPN, 826, 842
  NetBIOS inspection, 406
  NetFlow, 12
  Netmask attribute (ASDM), 209
  network access, controlling
    address translation
      bypassing, 218-221
      configuring, 206-216
      interface security levels, 203
      ISN randomization, 204
      monitoring, 229-230
      NAT, 200-201, 207-211, 216-224
      packet flow sequences, 204
      PAT, 202, 212-216
      TCP interception, 205-206
    content filtering, 173-175
      enabling via Websense, 190-192
      monitoring, 198
DNS doctoring, 225-228
monitoring ACL, 193-197
packet filtering, 142-146
traffic filtering, 147-158
   enabling content filtering via Websense, 190-192
   filtering inbound traffic via ACL, 185-189
URL filtering, 175-178
   buffering server responses, 182
caching server responses, 184
   enabling long URL support, 184
   FTP filtering, 180-182
   HTTP filtering, 180-182
   HTTPS filtering, 180-182
Network ACL tab (ASDM), DAP configurations, 1012
network activity tests (failover interface tests), 524
network firewalls
   application proxies (proxy servers), 3
   NAT, 3
      PAT, 4
      static translation, 5
   packet-filtering, 2-3
network-based object groups, 160
new pin mode, 316
NIDS (Network Intrusion Detection System), 10
NIPS (network intrusion prevention systems), 8
NSEL (NetFlow Secure Event Logging), 125
   NetFlow Collector, defining, 126-127
   NetFlow export policy, defining, 127-128
NSSA (Not-So-Stubby Areas), OSPF, 268
   authentication, 262-267, 279
dynamic routing over VPN, 270-272
   enabling, 254-258
neighbor command, 270-271
NSSA, 268
redistribution, 266-267
stub areas, 267
troubleshooting
   authentication mismatches, 279
   commands, 273-278
NTP (Network Time Protocol), automatic system clock adjustments, 86
NVRAM (Non-Volatile Random Access Memory), password recovery process, 108-109, 113
object grouping, 159
   ACL, 164-166
   ICMP-type groups, 160
   network-based groups, 160
   object types, configuring, 160-162
   protocol-based groups, 160
   service-based groups, 160
one-time upgrades, applying to AIP-SSM, 638-639
operator account (AIP-SSM), 632
options (commands), displaying supported options in, 54
Original Interface attribute (ASDM), 207
Original Port attribute (ASDM), 213
Original Source attribute (ASDM), 207
OSPF (Open Shortest Path First), 252-253
   authentication, 262-267, 279
dynamic routing over VPN, 270-272
   enabling, 254-258
neighbor command, 270-271
NSSA, 268
redistribution, 266-267
stub areas, 267
troubleshooting
   authentication mismatches, 279
   commands, 273-278
mismatched areas, 279
virtual links, 279
Type 3 LSA filtering, 268-270
updates over IPsec, site-to-site IPsec
VPN, 755-756
virtual links, 259-261, 264-267
VPN tunneling, 272
OTP (one-time passwords), 316
outgoing SMTP scanning (CSC SSM),
configuring, 704

P

packets
capturing, 136-138, 196
classification
QoS, 583-587
security contexts, 421-422
shared interface criteria,
422-424
filtering
ACE, 142-143, 147-154, 158
ACL, 2-3, 142-152
network firewalls, 2-3
traffic filtering, 147-158,
185-192
flow
MMTF, 477
multiple mode (security
contexts), 424-426
sequences, address translation,
204
SMTF, 474-476
tracing, 136
fragmentation, site-to-site IPsec
VPN, 767-768
troubleshooting
capturing packets, 136-138
monitoring dropped packets,
138-139
tracing packet flows, 136
partial commands, completing, 54
passwords
AIP-SSM users, changing passwords
for, 635-636
CSC SSM, recovering on, 722-724
device passwords, ASA device setup,
67-68
OTP, 316
recovery process, 106-109, 113
PAT (Port Address Translation), 202
dynamic PAT, 214-215
network firewalls, 4
PAT mode (Easy VPN), 826
policy PAT, 216
static PAT
configuring, 213-214
port redirection, 212
pattern matching
false positives, 10
IDS, 9-10
signatures, 9
stateful pattern-matching
recognition, 10
peer-id-validate cert command, 908
periodic function (time-based ACL),
168
personal firewalls, 2, 7
PFS (Perfect Forward Secrecy)
Diffie-Hellman exchanges, 19
site-to-site IPsec VPN, 761
phone proxy, UC advanced support,
383-388
PIM (Protocol Independent Multicast)
multicast routing
enabling PIM in, 305
filtering PIM neighbors, 307
PIM-DM (dense mode), 302
PIM-SM (sparse mode), 302
ping tests (broadcast), 524
PKI (public key infrastructure), 869
CA, 871-872
certificates
   accepting remote-access IPSec
      VPN clients, 910-916
   configuring IPSec site-to-site
tunnels, 906-910
explained, 870-871
installing, 874-896
CRL, 873
Local CA
   configuring, 896-901
   enrolling users, 901-905
SCEP, 874
troubleshooting, 917
   CRL retrieval, 921
   SCEP enrollment, 920-921
   time and date mismatch,
      917-920
plug-ins (client-server), clientless SSL
VPN configurations, 979
policy maps
   application inspection, 352
   QoS configurations, 598-600
policy NAT (Network Address
Translation), 216
policy PAT (Port Address Translation),
216
Pool ID attribute (ASDM), 209
POP3 support (CSC SSM),
configuring, 709
port forwarding
Port Forwarding Lists tab (ASDM),
DAP configurations, 1015
SSL VPN configuration, 974
   defining port-forwarding lists,
      975
   mapping port forwarding lists
to group policies, 976
port redirection (static PAT), 212
port-misuse command, HTTP
inspection, 396
portal customization, SSL VPN
configuration, 949
full customizations, 960-964
logon page, 958-962
   banner area, 951
   copyright area, 953
   information area, 953
   logon area, 952
logout page, 957
portal page, 955-956, 960, 963-964
user connection profiles, 960
user groups, 957-959
portal page (SSL VPN)
   content area, 956
   customizing, 963-964
   navigation panel, 955-956
   title panel, 955
   toolbar, 955
   user connection profiles, 960
PPTP (Point-to-Point Tunneling
Protocol)
inspection, 406
VPN, 13
prelogin sequences (CSD)
   Cache Cleaner policies,
      996-997
   CSD policies, assigning, 990
host emulators, identifying, 990-991
keystroke loggers, identifying, 990-991
prelogin policies, 987-989
Secure Desktop (Vault) attributes, 992-995, 998
Presence Federation Proxy, UC advanced support, 390
preshared keys, site-to-site IPSec VPN, 795-797
Preview Commands Before Sending Them to the Device option (ASDM), 67
priority queues, QoS configurations
ASDM, 589
CLI, 597
Privileged mode (CLI), 53
privileges (user), CSD, 983
Profile Editor, creating AnyConnect SSL VPN client profiles, 1056
profile-based detection, IDS, 11
promiscuous IPS mode, traffic flow, 618
Properties icon (ASDM Monitoring screen), 67
protocol analysis (protocol decode-base signatures), NIDS, 10.
See also stateful pattern-matching recognition
Protocol attribute (ASDM), 213
protocol-based detection, IDS, 11
protocol-based object groups, 160
proxy servers (application proxies), network firewalls, 3

Q

QIL (Quick IP Lookup), 706
QoS (Quality of Service), 577
ASDM configurations
applying action rules, 593-595
defining service policies, 589
priority queues, 589
specifying traffic selection criteria, 590-592
CLI configurations
class maps, 597-598
policy maps, 598-600
priority queues, 597
deleting
remote-access VPN tunnels, 607-610
VoIP, 600-606
monitoring, 611-612
packet classification
ACL, 586
IP DSCP field, 583-586
IP flow, 587
IP Precedence field, 583
VPN tunnel groups, 587
packet flow sequence, 582
security appliance compatibility, 578
traffic policing, 579-580, 594
traffic prioritization, 579, 593
traffic shaping, 581, 595
VPN tunneling, 588
remote-access VPN tunnel deployments, 607-610
VPN tunnel groups, 587
queries, IGMP query timeouts, 304
question mark (?), displaying command help in CIPS CLI, 626
quick mode (IPSec), 18
RADIUS, 314
  accounting, 341
  user authentication
    AnyConnect SSL VPN, 1061
    defining RADIUS for IPSec
      authentication, 945-946, 1040
    SSL VPN configurations,
      943-946, 1038-1040
  RAs (registration authorities), 872
  RAS (Registration, Admission, and Status) protocol, H.323, 378
RBL (Real-time Blacklist), 706
re-imaging CSC SSM, 719-721
recovering passwords on CSC SSM, 722-724
redistribution (route)
  EIGRP, 289-291
  OSPF, 266-267
  RIP, 249
redundancy
  device-level redundancy
    Active/Active redundancy,
      528-531, 540-548, 553-554, 564-568
    Active/Standby redundancy,
      527-528, 534-540, 552-553, 560-564
  interface-level redundancy
    multiple-mode firewalls, 551
    redundant interface guidelines,
      531-533
    single-mode firewalls, 550
registration authorities (RAs), 872
registry checks, 989
remote access clients, ASDM configurations
  IPSec remote-access VPN, 822
  L2TP over IPSec remote-access VPN, 846
Remote Access VPN icon (ASDM Configuration screen), 65
remote system management
  SSH, 98-101
  Telnet, 95-97
remote-access VPN (virtual private networks), 13-15
  advanced features, 836
  IPSec remote-access VPN, 800, 840-842
    accepting clients via certificates, 910-916
    ASDM configuration, 822-823
    assigning IP addresses, 812-816
    bypassing NAT (optional), 818
    configuring user authentication, 810-812
    creating ISAKMP policies, 803-804
    crypto maps, 816-817
    defining IPSec policies, 809
    deployment scenarios, 849-860
    DNS (optional), 821
    enabling ISAKMP, 802-803
    hardware-based VPN client configurations, 826-828
    IPSec hairpinning, 831
    L2TP over IPSec remote-access VPN versus, 800
    load balancing, 849-855
    setting up group policies, 806
    setting up tunnel groups, 808
software-based VPN client configurations, 824
split tunneling (optional), 818-819
traffic filtering (optional), 817-818
transparent tunneling, 829-831
troubleshooting, 867
tunnel default gateways, 828
VPN client firewalls, 836-838
VPN load balancing, 833-835
WINS (optional), 821
L2TP over IPSec remote-access VPN, 843
ASDM configuration, 846-848
IPSec hairpinning, 856-860
IPSec remote-access VPN over, 800
Windows client configuration, 848
monitoring, 860-864
troubleshooting, 865-867
tunnels, QoS deployments
ASDM configurations, 607-608
CLI configurations, 609-610
remote-management protocols, SSH, 99
request-method command, 396-398
resource management, security contexts, 439-442
resource member classes, defining (security contexts), 440-442
retiring signatures (IPS), 680-681
reverse proxies, 22-23
revoking certificates, 873
RIP (Routing Information Protocol), 240
authentication, 244, 251
configuring, 241-243
redistribution, 249
route filtering, 246-248
troubleshooting
  authentication mismatches, 251
  blocked multicast/broadcast packets, 251-252
  version mismatches, 250
ROMMON (Read-Only-Memory Monitor), 54
image recovery, 105
password recovery process, 106, 109-111
route filtering
  EIGRP, 284
  RIP, 246-248
route redistribution
  EIGRP, 289-291
  OSPF, 266-267
  RIP, 249
route summarization, EIGRP, 287
routed firewalls, 471
  enabling, 484
  transparent firewalls versus, 472-474
routed mode (interface configuration), 70
router advertisement transmission intervals (IPv6), 83
routing
  ABR routers, 252
  asymmetric routing, Active/Active failovers, 529-531, 547
dynamic routing over VPN, OSPF, 270-272
EIGRP
  authentication, 285, 300
  controlling default information, 291-292
defining static neighbors, 286-287
enabling, 280-284
route filtering, 284
route redistribution, 289-291
route summarization, 287
split horizon, 288
troubleshooting, 292-300

multicast routing
configuring RP, 306
defining IGMP version, 304
enabling, 302
enabling PIM, 305
filtering PIM neighbors, 307
GMP stub mode, 301
IGMP query timeouts, 304
limiting IGMP states, 303-304
PIM-SM, 302
static multicast routes, 307-308
statically assigning IGMP groups, 302
troubleshooting, 308-310

OSPF, 252
authentication, 262-267, 279
dynamic routing over VPN, 270-272
enabling, 254-258
neighbor command, 270-271
NSSA, 268
redistribution, 266-267
stub areas, 267
troubleshooting, 273-279
Type 3 LSA filtering, 268-270
virtual links, 259-261, 264-267
VPN tunneling, 272

RIP, 240
authentication, 244, 251
configuring, 241-243
redistribution, 249
route filtering, 246-248
troubleshooting, 250-252

static routing, 231-233
displaying routing tables, 239-240
monitoring, 234-235, 238

Routing icon (ASDM Monitoring screen), 67
routin...ing, 272, 757-758, 775-789

RSA keys
digital certificate requests, 933, 936
digit... pair, generating in CLI, 883-884
RSA SecureID (SDI), 316-317
RSH (Remote Shell) inspection, 407
RTCP (Real-Time Transport Control Protocol), H.323, 377
RTO (retransmission timeouts), 293
RTSP (Real-Time Streaming Protocol) inspection, 408
running configurations, 88-91, 94

S

SCCP (Simple Client Control Protocol) inspection, 410-411
SCEP (Simple Certificate Enrollment Protocol), 874
certificates, installing from, 878-883
enrollment, troubleshooting PKI, 920-921
scheduled upgrades, configuring for AIP-SSM, 639, 642-643
SDEE (Security Device Event Exchange), 619
SDI (SecureID), 316-317
Secure Desktop (Secure Session), 982, 992-995, 998
Secure Desktop Manager, 982
Secure PIX Firewall (Cisco), cut-through proxy feature, 330-333
authentication
  customizing prompts, 335-336
timeouts, 335
troubleshooting firewall sessions, 347
secure unit authentication. See interactive client authentication
SecureMe
  AnyConnect SSL VPN deployments, 1059
clientless SSL VPN deployments, 1017-1020
security
  encryption
    ACL, 747
    AES, 737
firewalls
  authentication, 330-336
cut-through proxy feature (Cisco Secure PIX Firewall), 330-336, 347
troubleshooting sessions, 347
live security event messages (CSC SSM), monitoring, 717
passwords, OTP, 316
signatures, customizing, 651-656
security contexts
  admin context, 418-419
    ASDM configuration using shared interfaces, 458
    configuring, 435-436
    MMTF deployments, 505-506
  configuring, 417
    admin context configuration, 435-436
    allocate interfaces, 433
    context descriptions, 432
    enabling multiple security contexts globally, 427-429
    reverting to single-mode firewall, 429
    setting up system execution space, 430-432
    specifying configuration URL, 434-435
    user context configuration, 437
    verifying virtual firewall mode, 429
deploying using non-shared interfaces, 443
  ASDM configurations, 445-450
  CLI configurations, 451-454
deploying using shared interfaces, 454
  ASDM configurations, 456-462
  CLI configurations, 462-466
managing, 438
MMTF deployments, 502
  ASDM deployments, 504-510
  CLI deployments, 510-514
monitoring, 466-467
packet classification, 421
  non-shared interface criteria, 422
  shared interface criteria, 422-424
packet flow in multiple mode
forwarding with shared interfaces, 425-426
forwarding without shared interfaces, 424
removing, 438
resource management, 439
defining resource member classes, 440-442
mapping member classes to contexts, 442
support for, 417
system execution space, 418
adding user contexts to, 432
ASDM configuration using non-shared interfaces, 445
ASDM configuration using shared interfaces, 456-457
available options table, 417
MMTF deployments, 504-505
monitoring output of, 466-467
setting up, 430-432
troubleshooting
adding new contexts, 468
connectivity issues with shared security contexts, 469-470
saving contexts on FTP servers, 469
saving contexts to local disks, 468
user context, 419
adding to system execution space, 432
allocating interfaces, 433
ASDM configuration using non-shared interfaces, 447-450
ASDM configuration using shared interfaces, 458-462
configuring, 437
MMTF deployments, 507-510
verifying number of, 419-421
uses of, 415
selective application inspection, 353-354
SensorApp (CIPS), 621-622
serial console connections, authentication, 329
service account (AIP-SSM), 633
Service attribute (ASDM), 153, 156
service packs, applying to CIPS, 637
service policies
application inspection, 352-356
QoS configurations via ASDM, 589
service-based object groups, 160
session command, 616
setup command, 627-631
Shared Premium licenses, 928-929, 1029-1030
show clock command, 918
show commands
multicast routing, troubleshooting, 308-309
show configuration command, 645-646
show crypto ca certificates command, 888, 918
show crypto ca crls command, 895
show crypto ca server certificate command, 901
show crypto ca server command, 900
show crypto ca server user-db allowed command, 905
show crypto ca server user-db command, 905
show crypto ca server user-db enrolled command, 905
show crypto ca server user-db
expired command, 905
show crypto ca server user-db
on-hold command, 905
show crypto ca server user-db
username command, 905
show crypto key mypubkey rsa
command, 884
show events command, 648-649
show firewall command, 484
show module command, 616
show statistics analysis-engine
command, 684-685
show statistics authentication
command, 685
show statistics command, 684-687
show statistics event-server
command, 685
show statistics event-store command,
686
show statistics host command,
686-687
show statistics logger command, 687
show version command, 643-644
Show System Information tool (CSC
SSM), 727-733
shunning, configuring on AIP-SSM,
659-662
signatures
customizing, 651-656
disabling, 679-680
pattern matching, 9
retiring, 680-681
single-mode firewalls
interface-level redundancy, 550
multiple-mode firewalls versus,
419-421
SIP (Session Initiation Protocol),
inspection, 408-410
site-local addresses, IPv6
configuration, 82
site-to-site IPSec VPN (Virtual Private
Networks), 13, 735
configuring
bypassing NAT (optional), 751
Connection Profiles, 753-755
creating ISAKMP policies,
739-740
crypto maps, 745-749
defining IPSec policies, 743-745
enabling ISAKMP, 739
IPSec VPN Wizard, 752-753
preconfiguration checklist,
736-737
setting up tunnel groups,
741-743
traffic filtering (optional),
749-750
connection types, 764-765
deploying
fully meshed topologies with
RRI, 775-789
single site-to-site tunnel
configuration via NAT
Traversal, 769-775
keepalives feature (ISAKMP), 766
management access, 760
monitoring, 789-792
NAT Traversal, 758-759
OSPF updates over IPSec, 755-756
packet fragmentation, 767-768
PFS, 761
Phase 1 mode, 764
RRI, 757-758, 775-789
security association lifetimes,
763-764
Site-to-Site VPN icon (ASDM Configuration screen), 65
troubleshooting, 793-794
  incompatible IPSec transform sets, 796
ISAKMP captures, 797-798
ISAKMP proposal unacceptable, 795
mismatched preshared keys, 795
mismatched proxy identities, 796-797
tunnel default gateways, 759-760
Skinny (SCCP) inspection, 410-411
smart tunnels, SSL VPN configuration, 976-978
SMTF (single-mode transparent firewalls)
deploying, 496
  ASDM deployments, 498-500
  CLI deployments, 501-502
packet flow, 474-476
SMTP (Simple Mail Transfer Protocol)
Content Filtering (CSC SSM), configuring, 708-709
ESMTP, application inspection, 363-366
scanning (CSC SSM)
  Anti-spam Content Scanning, 704-706
  Anti-spam Email Reputation, 706-708
configuring, 701
incoming messages, 701-704
SNMP (Simple Network Management Protocol), 128
configuring, 130-133
inspection, 411-412
monitoring, 133
software
installing
  image recovery via ROMMON, 105
  image upgrades via ASA CLI, 102-104
  image upgrades via ASDM, 101
SSL VPN software requirements, 930, 1032-1033
upgrades, performing on CSC SSM, 726
zero-downtime software upgrades (failovers), 557-559
Source attribute (ASDM), 153, 156, 220
Source Service attribute (ASDM), 153, 156
spam, Anti-spam Content Scanning (CSC SSM), 704-706
sparse mode (PIM-SM), 302
SPF (Shortest Path First) algorithm, 252
split horizon, EIGRP, 288
split tunneling
  AnyConnect SSL VPN, 1049-1051
  IPSec remote-access VPN, 818-819
SQL*Net inspection, 412
SRTT (smooth round-trip time), 293
SSH (Secure Shell), 98-101
authentication, 327-328
known host list, 637
SSL VPN (Secure Socket Layer Virtual Private Network), 13, 23, 923
ActiveX support, 930
administrative privileges, 931, 1034
AnyConnect SSL VPN, 1027
configuring, 1040-1061
deploying, 1059-1062
monitoring, 1063
Standalone mode, 1042
troubleshooting, 1063-1065
VPN client versus, 1028
Web-enabled mode, 1041
ASA feature set, 925, 1031
ASA placement, 931, 1034
browser support, 930, 1032-1034
client-based SSL VPN, 1027
configuring, 1040-1061
deploying, 1059-1062
monitoring, 1063
Standalone mode, 1042
troubleshooting, 1063-1065
VPN client versus, 1028
Web-enabled mode, 1041
clientless mode
configuring, 947-979
deployment scenarios,
1017-1020
enabling on an interface, 949
monitoring, 1021-1023
troubleshooting, 1024-1026
VPN client versus, 924
configuring
application access, 973-978
bookmarks, 965-969
client-server plug-ins, 979
digital certificate enrollment,
931-936, 1035
enabling clientless SSL VPN on
an interface, 949
group policies, 937-941, 1035-1036
logon page customization,
951-953, 958-962
logout page customization, 957
port forwarding, 974-976
portal customization, 949-964
portal page customization,
955-957, 960, 963-964
smart tunnels, 976-978
tunnel policies, 937, 941-942,
1035-1037
user authentication, 943-946,
1038-1040
web-type ACL, 970-973
design considerations
clientless SSL VPN versus VPN
client, 924
implementation scope,
925, 1031
infrastructure planning,
925, 1031
system demands, 925, 1031
user connectivity, 924-926
full tunnel mode, 924, 1027
configuring, 1040-1061
deploying, 1059-1062
monitoring, 1063
Standalone mode, 1042
troubleshooting, 1063-1065
VPN client versus, 1028
Web-enabled mode, 1041
HTTPS, 21-22
infrastructure requirements,
931, 1034
licenses, 926
AnyConnect Essentials
licenses, 928, 1028-1030
AnyConnect Mobile licenses,
928, 1029-1030
AnyConnect Premium licenses,
928, 1028-1030
device associations, 929
Shared Premium licenses, 928-929, 1029-1030
VPN Flex licenses, 929, 1030
software requirements, 930, 1032-1033
Sun JRE support, 930
supported operating systems, 930, 1032-1033
thin client mode, 924
user account requirements, 931, 1034
web folder support, 930
SSO (single sign-on) authentication, 318
servers, clientless SSL VPN configurations, 969
Standalone mode (AnyConnect SSL VPN), 1042
standard ACL (access control lists), 144, 166
standby appliances (failover), 521
Starting IP Address attribute (ASDM), 209
startup configurations, 92-94
State Limit feature (IGMP), 303-304
state tables, 6
stateful failover, 524-526
  Active/Active failovers, 542-543
  Active/Standby failovers, 538-539
stateful inspection firewalls, 6
stateful links, 525
stateful pattern-matching recognition, 10. See also protocol analysis
stateless failover, 524
static L2F tables, adding entries to transparent firewalls, 492
static multicast routing, 307-308
static NAT (Network Address Translation), 207
static PAT (Port Address Translation) configuring, 213-214
port redirection, 212
static routing, 231-232
displaying routing tables, 239-240
monitoring, 234-235, 238
static translation, network firewalls, 5
statistics, displaying for AIP-SSM, 684-687
stealth firewalls. See transparent firewalls
storing system logs internally/externally
  Flash logging, 123
  FTP logging, 124
strict-http command, HTTP inspection, 393
stub areas, OSPF, 267
stub mode (GMP), 301
Sub-configuration mode (CLI), 53
subinterface, configuring (ASA device setup), 73-74
summarization (route), EIGRP, 287
Sun JRE (Java Runtime Environment), SSL VPN support, 930
Sun RPC (Remote Procedure Call) protocol inspection, 407
SVC (SSL VPN Client), 1040, 1065
ten (commands), displaying, 54
Syslog
  configuring for CSC SSM, 718-719
  enabling via ASDM, 115
  message ID tuning, 124
  server logging, 119
  servers, defining, 121-122
system clocks
  automatic adjustments via NTP, 86
manual adjustments
  dates/times, 85
time zones, 84
system execution space (security contexts), 418
ASDM configuration using
  non-shared interfaces, 445
  shared interfaces, 456-457
available options table, 417
MMTF deployments, 504-505
monitoring output of, 466-467
setting up, 430-432
user contexts, adding, 432
system information, displaying, 54-55
system maintenance
  password recovery process, 106-113
  software installation
  image recovery via ROMMON, 105
  image upgrades, 101-104
system monitoring
  NSEL, 125
  defining NetFlow Collector, 126-127
  defining NetFlow export policy, 127-128
SNMP, 128-133
system logging, 113
ASDM logging, 119
buffered logging, 119-121
console logging, 118
defining email servers, 122
defining event lists, 116-117
defining Syslog servers, 121-122
email logging, 119
enabling, 114-115
setting up logging lists, 120-121
storng logs internally/externally, 123-124
Syslog message ID tuning, 124
Syslog server logging, 119
terminal logging, 119
System Resources Status section (ASDM Home screen), 64

T

T.38 protocol, 382
tables
  routing tables, displaying, 239-240
  state tables, 6
TACACS+, 316
  accounting, 343
  authorization, 338
TCP (Transfer Control Protocol)
  interception, 205-206
  IPSec over UDP, IPSec remote-access VPN, 831
Telnet, 95-97, 325-327
terminals
  H.323, 376
  logging, 119
testing
  ARP tests, 524
  broadcast ping tests, 524
  failover interface tests, 523-524
  link up/down tests, 523
  network activity tests, 524
TFTP (Trivial File Transfer Protocol)
  image recovery, 105
  inspection, 412
thin client mode (SSL VPN), 924
thru-traffic filtering
ASDM, 152-154
CLI
  ACL setup, 147-151
  applying ACL to an interface, 151-152
time/date
mismatches, troubleshooting PKI, 917-920
system clocks
  manual adjustments, 85
time zones, 84
time mode (authentication servers), 323
Time Range attribute (ASDM), 154-156
time-based ACL (access control lists), 167, 170
  absolute function, 168
  periodic function, 168
time-range configuration, 169
title panel (SSL VPN portal page), customizing, 955
TLS known host list, 637
TLS proxy, UC advanced support, 388-389
TLS trusted hosts, adding to AIP-SSM, 637
to-the-box-traffic filtering, 154-156
toolbar (SSL VPN portal page), customizing, 955
traffic classification, configuring for Cisco ASA Botnet Traffic Filter feature, 672-673
Traffic Direction attribute (ASDM), 153
traffic filtering
  AnyConnect SSL VPN configurations, 1054
deployment scenarios
  enabling content filtering via
    Websense, 190-192
  filtering inbound traffic via
    ACL, 185-189
  IPSec remote-access VPN, 817-818
  IPv6 ACL setup, 157-158
  packet filtering, 147-158, 185-192
  site-to-site IPSec VPN, 749-750
  thru-traffic filtering
    ASDM, 152-154
    CLI, 147-152
to-the-box-traffic filtering, 154-156
traffic policing, 579-580, 594
traffic prioritization, 579, 593
traffic shaping, 581, 595
Traffic Status section (ASDM Home screen), 64
TransactionSource, 625
transfer-encoding type command, HTTP inspection, 398
Translated Interface attribute (ASDM), 207
Translated Port attribute (ASDM), 213
Translated Use IP Address attribute (ASDM), 207
transparent firewalls, 471
configuring
  adding static L2F table entries, 492
  ARP packets, 488
  BPDUs, 488
  CDP packets, 487
  enabling ARP inspection, 492-494
  enabling transparent firewalls, 483
guidelines for, 482
interface ACL, 487-489
IP addresses, 485
L2F table aging time, 496
MPLS, 488
NAT, 491
setting up default gateways, 487
setting up interfaces, 484
setting up routes, 486
MMTF
deploying, 496
deploying with security contexts, 502-514
packet flow, 477
monitoring, 514-516
NAT, 479-481
restrictions within, 479-481
routed firewalls versus, 472-474
SMTF
deploying, 496-502
packet flow, 474-476
troubleshooting, 516-519
VPN, 479
transparent tunneling, IPSec
remote-access VPN
IPSec over TCP, 831
IPSec over UDP, 830
NAT-T, 829-830
Transport mode (IPSec), 20
Trend Micro Content Security icon
(ASDM Monitoring screen), 67
Trend Micro website, 707
troubleshooting
administrative connections, authentication, 344-347
AnyConnect SSL VPN
connection issues, 1064-1065
SSL negotiations, 1063
clientless SSL VPN
CIFS issues, 1024-1025
CSD, 1025
DAP, 1025-1026
SSL negotiations, 1024
website issues, 1024
CPU, 139
CSC SSM
installation issues, 722
password recovery, 722-724
CSD, 1025
DAP, 1025-1026
EIGRP
authentication, 300
commands, 292-295
hello intervals, 297-300
hold intervals, 297-300
link failures, 296-297
failovers, 572-574
firewall sessions, cut-through proxy feature (Cisco Secure PIX Firewall), 347
multicast routing
debg commands, 309-310
show commands, 308-309
OSPF
authentication mismatches, 279
commands, 273-278
mismatched areas, 279
virtual links, 279
packet issues
capturing packets, 136-138
monitoring dropped packets, 138-139
tracing packet flows, 136
PKI, 917
  CRL retrieval, 921
  SCEP enrollment, 920-921
time and date mismatch, 917-920
remote-access VPN, 865-867
RIP
  authentication mismatches, 251
  blocked multicast/broadcast packets, 251-252
  version mismatches, 250
security contexts
  adding new contexts, 468
  connectivity issues with shared security contexts, 469-470
  saving contexts on FTP servers, 469
  saving contexts to local disks, 468
site-to-site IPSec VPN, 793-794
  incompatible IPSec transform sets, 796
  ISAKMP captures, 797-798
  ISAKMP proposal unacceptable, 795
  mismatched preshared keys, 795
  mismatched proxy identities, 796-797
transparent firewalls, 516-519
troubleshooting tools (CSC SSM), 726
  Gather Logs, 733-734
  Management Port Console Access Settings, 734
  Show System Information, 727-733
trust-point command, 908
trusted hosts, adding to AIP-SSM, 636-637
trustpoints, configuring, 884-889
tuning
  AIP-SSM with CS-MARS, 683
  IPS, 677-681
tunneling
  default gateways
    IPSec remote-access VPN, 828
    site-to-site IPSec VPN, 759-760
  IPSec remote-access VPN
    ASDM configurations, 822
    setting up tunnel groups, 808
  L2TP over IPSec remote-access VPN
    ASDM configurations, 846
  split tunneling, IPSec remote-access VPN, 818-819
  transparent tunneling, IPSec remote-access VPN, 829-831
tunnel groups (connection profiles),
site-to-site VPN, 741-743
  Tunnel mode (IPSec), 20
tunnel policies, SSL VPN configurations,
  937, 941-942, 1035-1037
  VPN tunneling
    OSPF, 272
    QoS, 587-588, 607-610

U

UC (Unified Communications)
  advanced support
    Mobility Proxy, 389
    phone proxy, 383-388
    Presence Federation Proxy, 390
    TLS proxy, 388-389
UDP (User Datagram Protocol), IPSec over UDP, 830
updates, OSPF updates over IPSec, 755-756

upgrading

AIP-SSM

one-time upgrades, 638-639
scheduled upgrades, 639, 642-643
CSC SSM software, 726
images

ASA CLI, 102-104
ASDM, 101
zero-downtime software upgrades (failovers), 557-559

URL (uniform resource locators)

blocking (CSC SSM), 695-697
configuration URL, specifying in security contexts, 434-435
filtering, configuring, 175-177

buffering server responses, 182
caching server responses, 184
defining filtering servers, 178-180
enabling long URL support, 184
FTP filtering, 180-182
HTTP filtering, 180-182
HTTPS filtering, 180-182
Websense, 178-180

user accounts

AIP-SM

adding, 633-635
administrator account, 632
deleting, 633-635
operator account, 632
passwords, changing, 635
service account, 633
viewer account, 633

SSL VPN requirements, 931, 1034

user authentication

AnyConnect SSL VPN, 1061
IPSec remote-access VPN, 810-812

ASDM configurations, 822

Individual User Authentication, 841
L2TP over IPSec remote-access VPN, ASDM configurations, 847
SSL VPN configurations, 943-946, 1038-1040

user connectivity

connection profiles, clientless SSL VPN portal customization, 960
SSL VPN, 924-926

user context (security contexts), 419

allocating interfaces, 433
configuring, 437

ASDM configuration using non-shared interfaces, 447-450
ASDM configuration using shared interfaces, 458-462
MMTF deployments, 507-510
system execution space, adding to, 432
verifying number of, 419-421

user groups, clientless SSL VPN portal customization, 957-959

User mode (CLI), 52
user privileges, CSD, 983

V

Vault (Secure Desktop), CSD prelogin sequences, 992-995, 998
version of CIPS software, displaying, 643-644
viewer account (AIP-SSM), 633
Virtual Alarm, 622
virtual firewalls, deploying using
  non-shared interfaces, 443
    ASDM configurations, 445-450
    CLI configurations, 451-454
shared interfaces, 454
    ASDM configurations, 456-462
    CLI configurations, 462-466
virtual links, OSPF,
  259-261, 264-267, 279
Virtual Sensor, 622
VoIP (Voice over Internet Protocol),
  QoS deployments, 600
    ASDM configurations, 602-604
    CLI configurations, 605-606
VPN (Virtual Private Networks), 12
  dynamic routing over VPN, OSPF,
    270-272
Easy VPN
  Client (PAT) mode, 826
  IPSec remote-access VPN,
    824-828, 840-842
  NEM, 826, 842
Flex licenses, 929, 1030
GRE, 13
IPSec, 13-14
  Phase 1 negotiation, 15-17
  Phase 2 negotiation, 18-20
  quick mode, 18
IPSec remote-access VPN,
  800, 840-842
  ASDM configuration, 822-823
  assigning IP addresses,
    812-816
  bypassing NAT (optional), 818
  configuring user authentication, 810-812
  creating ISAKMP policies,
    803-804
  crypto maps, 816-817
  defining IPSec policies, 809
  deployment scenarios, 849-860
  DNS (optional), 821
  enabling ISAKMP, 802-803
  hardware-based VPN client configurations, 826-828
  IPSec hairpinning, 831
  L2TP over IPSec remote-access VPN versus, 800
  load balancing,
    833-835, 849-855
  monitoring, 860-864
  setting up group policies, 806
  setting up tunnel groups, 808
  software-based VPN client configurations, 824
  split tunneling (optional),
    818-819
  traffic filtering (optional),
    817-818
  transparent tunneling, 829-831
  troubleshooting, 865-867
  tunnel default gateways, 828
  VPN client firewalls, 836-838
  VPN load balancing, 833-835
  WINS (optional), 821
L2F, 13
L2TP, 13
L2TP over IPSec remote-access VPN,
  843
  ASDM configuration, 846-848,
    856-858
  CLI configuration, IPSec
  hairpinning, 858-860
  IPSec remote-access VPN over,
    800
MPLS, 13
NAT-T, 18
PPTP, 13
remote-access VPN, 13-15. See also
IPSec remote-access VPN, L2TP
over IPSec remote-access VPN
monitoring, 860-864
troubleshooting, 865-867
site-to-site IPSec VPN, 735
bypassing NAT (optional), 751
Connection Profiles, 753-755
collection types, 764-765
creating ISAKMP policies, 739-740
crypto maps, 745-749
defining IPSec policies, 743-745
enabling ISAKMP, 739
fully meshed topologies with
RRI, 775-789
IPSec VPN Wizard, 752-753
keepalives feature (ISAKMP), 766
management access, 760
monitoring, 789-792
NAT Traversal, 758-759
OSPF updates over IPSec, 755-756
packet fragmentation, 767-768
PFS, 761
Phase 1 mode, 764
preconfiguration checklist, 736-737
RRI, 757-758, 775-789
security association lifetimes, 763-764
setting up tunnel groups, 741-743

single site-to-site tunnel config-
uration via NAT Traversal, 769-775
traffic filtering (optional), 749-750
troubleshooting, 793-798
tunnel default gateways, 759-760
site-to-site VPN, 13
SSL, 13
SSL VPN, 21-23
transparent firewalls, 479
tunneling
OSPF, 272
QoS, 587-588, 607-610
VPN clients
accepting via certificates, 910-916
clientless SSL VPN versus, 924
firewalls, IPSec remote-access
VPN, 836-838
VPN icon (ASDM Monitoring
screen), 66
VPN Sessions section (ASDM Home
screen), 64

W

WAAS (Wide Area Application
Services) inspection, 413
watch lists, 663
web folders, SSL VPN support, 930
web-based features (CSC SSM)
configuring, 694
file blocking, 697-698
HTTP scanning, 699-701
URL blocking, 695-697
Web-enabled mode (AnyConnect SSL
VPN), 1041
web-type ACL (access control lists)
    defining, 972
SSL VPN configuration, 970-973
Web-Type ACL tab (ASDM), DAP configurations, 1013
webification, SSL VPN, 22
Websense
    content filtering, 190-192
    URL filtering, 178-180
websites
    clientless SSL VPN
        configuring, 966-967
        troubleshooting, 1024
Trend Micro, 707
Webtype ACL (access control lists), 146
Windows NT authentication, 317
WINS (Windows Internet Name Service)
    AnyConnect SSL VPN assignments, 1052
    IPSec remote-access VPN, 821
WINS (Windows Internet Naming Server) servers, defining, 968
wizards
    Failover Wizard (ASDM), configuring, 548-549
    IPSec VPN Wizard, site-to-site IPSec VPN, 752-753

X - Y - Z

X.509 standard, 870
XDMCP (X Display Management Control Protocol) inspection, 413
zero-day attacks, 12
zero-downtime software upgrades (failovers), 557-559
zones, 668