

Cisco ASA

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

Jazib Frahim, CCIE No. 5459

Omar Santos

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

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)	
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

- Authenticating Firewall Sessions (Cut-Through Proxy-Feature) 330
 - Authentication Timeouts 335
 - Customizing Authentication Prompts 335
- Configuring Authorization 336
 - Command Authorization 338
 - Configuring Downloadable ACLs 339
- Configuring Accounting 340
 - RADIUS Accounting 341
 - TACACS+ Accounting 343
- Troubleshooting Administrative Connections to Cisco ASA 344
- Troubleshooting Firewall Sessions (Cut-Through Proxy) 347
- Summary 347

Chapter 7 Application Inspection 349

- Enabling Application Inspection 351
- Selective Inspection 353
- Computer Telephony Interface Quick Buffer Encoding Inspection 356
- Distributed Computing Environment Remote Procedure Calls (DCERPC) 358
- Domain Name System 359
- Extended Simple Mail Transfer Protocol 363
- File Transfer Protocol 367
- General Packet Radio Service Tunneling Protocol 369
 - GTPvO 369
 - GTPv1 . 372 •
 - Configuring GTP Inspection 373
- H.323 376
 - H.323 Protocol Suite 376
 - H.323 Version Compatibility 378
 - Enabling H.323 Inspection 380 •, x
 - Direct Call Signaling and Gatekeeper Routed Control Signaling 382
 - T.38 382
- Unified Communications Advanced Support 383
 - Phone Proxy 383 •
 - TLS Proxy 388 »
 - Mobility Proxy 389 •• ;
 - Presence Federation Proxy 390 >

HTTP	390
Enabling HTTP Inspection	391
ICMP	399
ILS	399
Instant Messenger (IM)	400
IPSec Pass-Through	403
MGCP	404
NetBIOS	406
PPTP	406
SunRPC	407
RSH	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
 - Trouble shooting 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
Sensor App	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

Configuring CSC SSM Web-Based Features	694
URL Blocking and Filtering	695
File Blocking	697
HTTP Scanning	699
Configuring CSC SSM Mail-Based Features	701
SMTP Scanning	701
SMTP Anti-Spam	704
SMTP Content Filtering	708
POP3 Support	709
Configuring CSC SSM File Transfer Protocol (FTP)	709
Configuring FTP Scanning	709
FTP File Blocking	712
Summary	713
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

/

|
jj
A
j
|
I
J

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

|
\
/
\
J
i
?
>
->

	DAP Sequence of Events	1005
	Configuring DAP	1006
	Deployment Scenarios	1017
	Step 1: Define Clientless Connections	1019
	Step 2: Configure DAP	1020
	Monitoring and Troubleshooting SSL VPN	1021
	Monitoring SSL VPN	1021
	Troubleshooting SSL VPN	1024
	Summary	1026
Chapter 20	Client-Based Remote-Access SSL VPNs	1027
	SSL VPN Deployment Considerations	1028
	AnyConnect Licenses	1028
	Cisco ASA Design Considerations	1031
	SSL VPN Prerequisites	1032
	Client Operating System and Browser and Software Requirements	1032
	Infrastructure Requirements	1034
	Pre-SSL VPN Configuration Guide	1035
	Enrolling Digital Certificates (Recommended)	1035
	Setting Up Tunnel and Group Policies	1035
	Setting Up User Authentication	1038
	AnyConnect VPN Client Configuration Guide	1040
	Loading the AnyConnect Package	1042
	Defining AnyConnect SSL VPN Client Attributes	1044
	• Advanced Full Tunnel Features	1049
	• AnyConnect Client Configuration	1055
	• Deployment Scenario of AnyConnect Client	1059
	• Step 1: Set Up CSD For Registry Check	1061
	• Step 2: Set Up RADIUS for Authentication	1061
	• Step 3: Configure AnyConnect SSL VPN	1061
	• Step 4: Enable Address Translation for Internet Access	1062
	Monitoring and Troubleshooting AnyConnect SSL VPNs	1063
	Monitoring SSL VPN	1063
	• Troubleshooting SSL VPN	1063
	Summary	1066