

# Contents

Introduction	xix
Audience	xix
Audience Prerequisites	xix
What Is Covered	xx
Command Syntax Conventions	xxi
Device Icons Used in the Figures	xxi

## **Part I**      **Internet Security Fundamentals**    **3**

<b>Chapter 1</b>	<b>Internet Security</b>	<b>5</b>
	Internet Threats	5
	Network Services	6
	Router Services	6
	Firewall Services	8
	Authentication and Authorization Services	9
	Network Address Translation (NAT) Services	9
	Encryption and Decryption Services	10
	Proxy Services	11
	Security in the TCP/IP Suite	12
	Overview of TCP/IP	12
	Internet Protocol (IP)	14
	Address Resolution Protocol (ARP)	22
	Internet Control Message Protocol (ICMP)	23
	Transmission Control Protocol (TCP)	25
	User Datagram Protocol (UDP)	27
	Denial of Service (DoS) Attacks	27
	SYN Flood Attacks	28
	Ping Attacks	30
	Creating a Corporate Security Policy	30
	Summary	31
	Frequently Asked Questions	32
	Glossary	33

---

<b>Chapter 2</b>	<b>Basic Cisco Router Security</b>	<b>35</b>
	Basic Management Security	36
	Access Lists	37
	Standard Access Lists	39
	Extended Access Lists	43
	Named Access Lists	45
	Password Management	45
	The enable password Command	46
	The enable secret Command	47
	Physical Security	47
	Controlling Line Access	48
	Out-of-Band Management Security	49
	Cisco Discovery Protocol (CDP)	50
	Hypertext Transfer Protocol (HTTP) Configuration Services	51
	Simple Network Management Protocol (SNMP)	52
	Network Time Protocol (NTP)	55
	Banners	56
	Recommended Minimum IOS Security Settings	57
	Denying RFC 1918 Routes	57
	User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) Servers	58
	Finger Service	59
	IP Unreachables	59
	ICMP Redirect Messages	60
	Directed Broadcasts	62
	Proxy Address Resolution Protocol (ARP)	62
	IP Verify	63
	IP Source Routing	63
	TCP Intercept	64
	Summary	66
	Global Commands	67
	Interface Commands	68
	vty Commands	68

<b>Part II</b>	<b>Cisco Secure Product Family</b>	<b>71</b>
<b>Chapter 3</b>	<b>Overview of the Cisco Security Solution and the Cisco Secure Product Family</b>	<b>73</b>
	Cisco Security Solution	73
	Identity	74
	Perimeter Security	74
	Secure Connectivity	75
	Security Monitoring	75
	Security Management	76
	Cisco Secure Product Family	76
	Cisco Secure PIX Firewall	77
	Cisco IOS Firewall	78
	Cisco Secure Intrusion Detection System (IDS)	79
	Cisco Secure Scanner	81
	Cisco Secure Policy Manager	84
	Cisco Secure Access Control Server (ACS)	87
	Summary	88
	Frequently Asked Questions	88
	Glossary	89
	Bibliography	89
	URLs	90
<b>Chapter 4</b>	<b>Cisco Secure PIX Firewall</b>	<b>93</b>
	PIX Models	94
	PIX 506	94
	PIX 515	95
	PIX 520/525	96
	PIX 535	97
	PIX Features	98
	PIX Configuration	100
	Basic Configuration	100
	Realistic Configuration	108
	Single DMZ Configuration	114
	Dual DMZ with AAA Authentication	121
	VPN with Point-to-Point Tunneling Protocol (PPTP)	134
	ip local pool Command	135
	vpdn Command	136
	sysopt Command	137

---

	VPN with IPSec and Manual Keys	139
	crypto map Commands	140
	crypto ipsec Command	142
	VPN with Preshared Keys	144
	isakmp Commands	145
	Explanation of VPN with Preshared Keys	146
	Obtaining Certificate Authorities (CAs)	147
	PIX-to-PIX Configuration	148
	PIX-to-PIX with Identical Internal IP Addresses	150
	Summary	152
<b>Chapter 5</b>	Cisco IOS Firewall	155
	Access Lists	155
	Dynamic Access Lists	155
	Time-Based Access Lists	158
	Reflexive Access Lists	160
	Null Route	163
	Cisco IOS Firewall Features	165
	Port Application Mapping (PAM)	165
	How Context-Based Access Control (CBAC) Works	167
	CBAC Operation	168
	Sequence of CBAC Events	170
	Protocol Sessions Supported by CBAC	172
	Compatibility with Cisco Encryption Technology (CET) and IPSec	172
	Configuring CBAC	173
	Choose an Interface	174
	Configure IP Access Lists on the Interface	175
	Configure Global Timeouts and Thresholds	176
	Define Inspection Rules	177
	Configure Logging and Audit Trail	180
	CBAC Configuration Example	180
	Summary	182

<b>Chapter 6</b>	<b>Intrusion Detection Systems</b>	<b>185</b>
	Overview of Intrusion Detection	185
	Host-Based Intrusion Detection Systems	186
	Network-Based Intrusion Detection Systems	186
	Intrusion Detection Systems	188
	Cisco Secure Intrusion Detection System (CSIDS)	188
	Overview of the CSIDS Components	190
	The CSIDS Sensor	192
	The CSIDS Post Office Protocol	198
	The CSIDS Director	199
	Signatures	202
	Responding to Alarms	204
	Interpreting Logs	207
	Cisco IOS Firewall IDS	209
	Cisco Secure PIX Firewall IDS	210
	Cisco IDS Configuration	215
	Cisco IOS Firewall IDS Configuration	216
	Cisco Secure PIX Firewall IDS Configuration	218
	Summary	222
	Frequently Asked Questions	222
	Glossary	222
<b>Chapter 7</b>	<b>Cisco Secure Scanner</b>	<b>225</b>
	Cisco Secure Scanner Features	226
	Step 1: Network Mapping	226
	Step 2: Data Collection	230
	Step 3: Data Analysis	232
	Step 4: Vulnerability Confirmation	233
	Step 5: Data Presentation and Navigation	235
	Step 6: Reporting	238
	Cisco Secure Scanner Installation	241
	Cisco Secure Scanner Configuration	242
	Step 1: Running Cisco Secure Scanner	242
	Step 2: Creating a Session to Capture Data	243
	Step 3: Interpreting the Collected Data	247
	Step 4: Reporting on the Collected Data	249
	Summary	249

---

	Frequently Asked Questions	249
	Glossary	250
	URLs	250
<b>Chapter 8</b>	<b>Cisco Secure Policy Manager (CSPM)</b>	<b>253</b>
	CSPM Features	253
	CSPM Installation	255
	Hardware Requirements	256
	Software Requirements	256
	Planning your Installation	257
	Installation Procedures	264
	Configuration Example	269
	Configure the Network Topology	270
	Configure the Security Policy	291
	Generate and Publish the Device-Specific Command Sets	296
	Summary	299
	Frequently Asked Questions	299
	Glossary	299
	URLs	300
<b>Chapter 9</b>	<b>Cisco Secure Access Control Server (ACS)</b>	<b>303</b>
	Cisco Secure ACS Features	303
	Overview of Authentication, Authorization, and Accounting (AAA)	304
	Authentication	305
	Authorization	305
	Accounting	306
	RADIUS and TACACS+	307
	RADIUS	307
	TACACS+	308
	Differences Between RADIUS and TACACS+	309
	Cisco Secure ACS Installation	310
	Windows NT and Windows 2000 Installation	310
	UNIX Installation	311
	Cisco Secure ACS Configuration	313
	Web-Based Configuration and the ACS Admin Site	313
	User and Group Setup	315

- Network Configuration 318
- System Configuration 321
- Interface Configuration 323
- Administration Control 325
- External User Databases 327
- Reports and Activity 330
- Online Documentation 333

- Network Access Server Configuration 334
  - AAA Configuration Overview 334

- Configuration Example 340
  - Scenario 340
  - Technical Aspects 340
  - Potential Risks 341
  - Configuration 341
  - ACS Server Configuration 342
  - NAS Configuration 345
  - Authentication Configuration 345
  - Authorization Configuration 345
  - Accounting Configuration 347

- Summary 348

- Frequently Asked Questions 348

- Glossary 348

- Bibliography 349

- URLs 349

## **Part III Internet Security Situations 351**

### **Chapter 10 Securing the Corporate Network 353**

- Dial-In Security 353

- Dial-In User Authentication, Authorization, and Accounting (AAA) 356

- AAA Authentication Setup with TACACS+ and RADIUS 358

- Initial Configuration 359

- Building a Method List 360

- Linking the List to Interfaces 362

- Fine-Tuning the Configuration 364

- AAA Authorization Setup 364

- AAA Accounting Setup 366

---

Using All AAA Services Simultaneously	367
Virtual Private Networks (VPNs)	368
L2F	369
L2TP	369
Generic Routing Encapsulation (GRE) Tunneling	369
Encryption	369
IPSec Configuration	370
Summary	371
<b>Chapter 11</b> Providing Secure Access to Internet Services	<b>373</b>
Internet Services	374
Common Internet Security Threats	375
Network Intrusion	375
Denial of Service (DoS)	377
Internet Service Security Example	379
Initial Problems and Threats in the Internet Service Security Example	380
Proposed Changes to the Internet Service Security Example	381
Revised Problems and Threats in the Internet Service Security Example	385
Web Servers	386
Threats Posed to Web Servers	387
Solutions to the Threats to Web Servers	387
Configuration Recommendations for Web Servers	387
File Transfer Protocol (FTP) Servers	388
Threats Posed to FTP Servers	388
Solutions to the Threats to FTP Servers	389
Configuration Recommendations for FTP Servers	389
Internet e-Mail Servers (SMTP/POP3/IMAP4)	389
Threats Posed to Internet e-Mail Servers	390
Solutions to the Threats to Internet e-Mail Servers	391
Configuration Recommendations for Internet e-Mail Servers	391
Domain Name System (DNS) Servers	392
Threats Posed to DNS Servers	392
Solutions to the Threats to DNS Servers	393
Configuration Recommendations for DNS Servers	393
Back-End Servers	393
Threats Posed to Back-End Servers	394
Solutions to the Threats to Back-End Servers	394
Summary	394



Frequently Asked Questions 394

Glossary 395

## **Part IV      Appendix 397**

### **Appendix A    Cisco SAFE: A Security Blueprint for Enterprise Networks 399**

Authors of This Appendix 399

Abstract 399

Audience 400

Caveats 400

Architecture Overview 401

    Design Fundamentals 401

    Module Concept 402

    SAFE Axioms 404

Enterprise Module 410

    Expected Threats 410

Enterprise Campus 411

    Management Module 412

    Core Module 416

    Building Distribution Module 417

    Building Access Module 419

    Server Module 420

    Edge Distribution Module 422

Enterprise Edge 425

    Corporate Internet Module 426

    VPN and Remote-Access Module 432

    WAN Module 438

    E-Commerce Module 439

    Enterprise Options 444

Migration Strategies 444

Annex A: Validation Lab 445

    Overall Guidelines 446

    Management Module 449

    Core Module 451

    Building Distribution Module 452

    Building Access Module 452

    Server Module 453

    Edge Distribution Module 454

---

Corporate Internet Module	455
VPN and Remote-Access Module	457
WAN Module	460
Annex B: Network Security Primer	461
The Need for Network Security	461
Network Attack Taxonomy	461
What Is a Security Policy?	470
The Need for a Security Policy	471
Annex C: Architecture Taxonomy	471
References	472
RFCs	472
Miscellaneous References	473
Partner Product References	474
Acknowledgments	474
<b>Index</b>	<b>477</b>