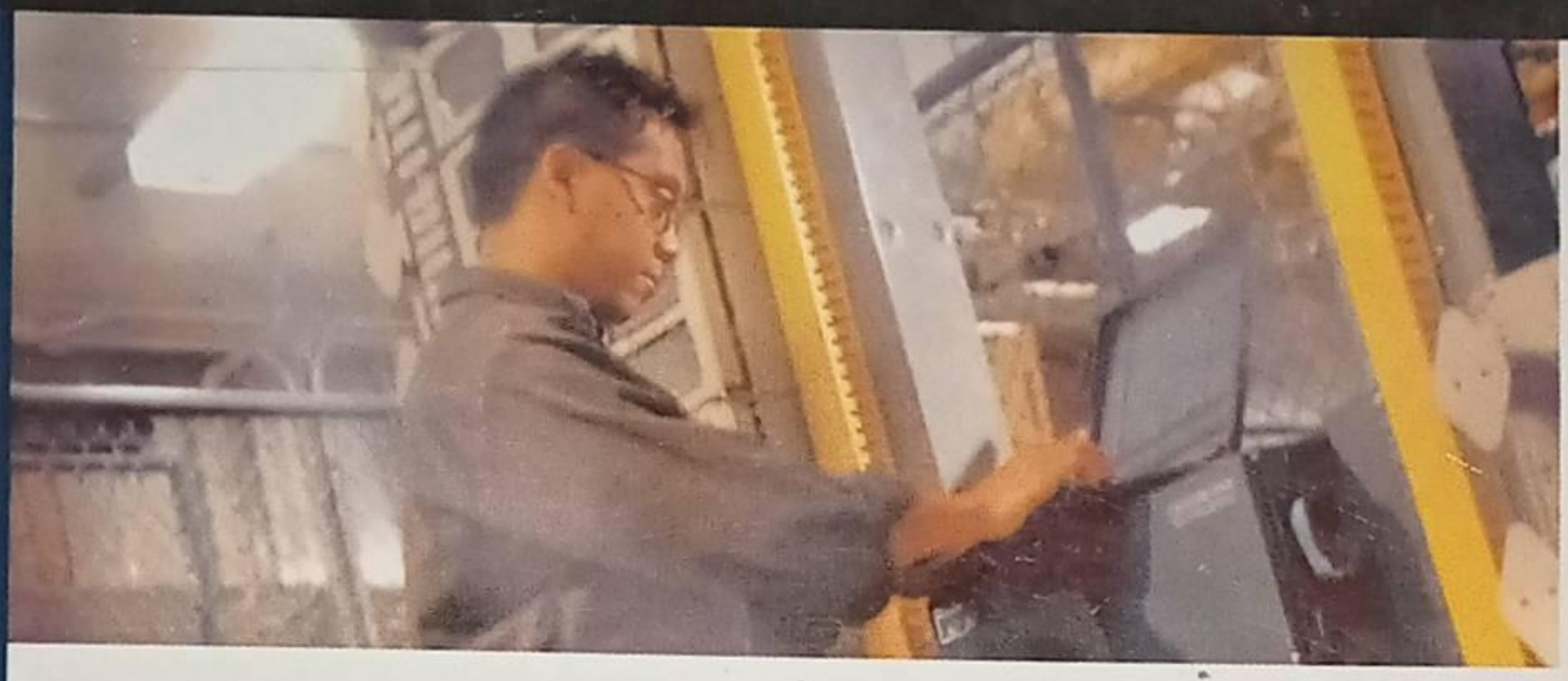
LOW PRICE EDITION

PEARSON Education

CISCO SYSTEMS



Network Security Architectures

Expert guidance on designing secure networks

Sean Convery, CCIE® No. 4232

ciscopress.com

Contents at a Glance

Foreword xxxiv

Preface xxxv

Part I **Network Security Foundations** 3

Chapter 1 Network Security Axioms 5

Chapter 2 Security Policy and Operations Life Cycle 29

Chapter 3 Secure Networking Threats 55

Chapter 4 Network Security Technologies 121

Part II **Designing Secure Networks** 169

Chapter 5 Device Hardening 171

Chapter 6 General Design Considerations 195

Chapter 7 Network Security Platform Options and Best Deployment Practices 269

Chapter 8 Common Application Design Considerations 299

Chapter 9 Identity Design Considerations 321

Chapter 10 IPsec VPN Design Considerations 353

Chapter 11 Supporting-Technology Design Considerations 413

Chapter 12 Designing Your Security System 449

Part III **Secure Network Designs** 479

Chapter 13 Edge Security Design 481

Chapter 14 Campus Security Design 535

Chapter 15 Teleworker Security Design 571

Part IV **Network Management, Case Studies, and Conclusions** 589

Chapter 16 Secure Network Management and Network Security Management 591

Chapter 17 Case Studies 635

Chapter 18 Conclusions 663

Appendix A Glossary of Terms 673

Appendix B Answers to Applied Knowledge Questions 679

Appendix C Sample Security Policies 699

Index 713

Table of Contents

Icons Used in This Book xxxii

Command Syntax Conventions xxxiii

Foreword xxxiv

Preface xxxv

Part I Network Security Foundations 3

Chapter 1 Network Security Axioms 5

Network Security Is a System 6

Business Priorities Must Come First 8

Network Security Promotes Good Network Design 10

Everything Is a Target 12

Everything Is a Weapon 14

Strive for Operational Simplicity 15

Good Network Security Is Predictable 19

Avoid Security Through Obscurity 21

Confidentiality and Security Are Not the Same 23

Summary 24

Reference 25

Applied Knowledge Questions 25

Chapter 2 Security Policy and Operations Life Cycle 29

You Can't Buy Network Security 30

What Is a Security Policy? 31

Security Policy Enforcement Considerations 32

Real-Time Technology Enforcement 32

Passive Technology-Assisted Compliance Checking 33

Nontechnical Compliance Checking 33

Contractual Compliance Checking 33

Next Steps 34

Security System Development and Operations Overview 34
Security System Development 35
Step 1: Examining Security Policy Drivers 36
Step 2: Developing a Security Policy 40
Step 3: Designing the Security System 44
Security System Operations Life Cycle 46
System Monitoring and Maintenance 46
Compliance Checking 48
Incident Response 49
Summary 50
References 50
Applied Knowledge Questions 51
Chapter 3 Secure Networking Threats 55
The Attack Process 56
Attacker Types 57
Script Kiddie 58
Cracker 59
Elite 59
Vulnerability Types 60
Software Vulnerabilities 60
Hardware Vulnerabilities 61
Configuration Vulnerabilities 61
Policy Vulnerabilities 62
Usage Vulnerabilities 62
Attack Results 62
Disclosure of Information 63
Corruption of Information 63
Denial of Service 63
Theft of Service 63
Increased Access 63
Attack Taxonomy 64
Read 69
Reconnaissance 69
Sniffer 75
Direct Access 77

Manipulate 78
Network Manipulation 78
Application Manipulation 79
Spoof 82
MAC Spoofing 83
IP Spoofing 84
Transport Spoofing 86
Identity Spoofing 90
Rogue Devices 92
Flood 94
MAC Flooding 94
Network Flooding 95
TCP SYN Flooding 100
Application Flooding 102
Redirect 103
L2 Redirection 103
IP Redirection 105
Transport Redirection 106
Composite 107
Man-In-The-Middle 108
Viruses, Worms, and Trojan Horses 110
Rootkit 112
Remote Control Software 113

Summary 115

References 117

Applied Knowledge Questions 118

Chapter 4 Network Security Technologies 121

The Difficulties of Secure Networking 121

Security Technologies 126
Identity Technologies 126
Reusable Passwords 127
RADIUS and TACACS+ 128
OTPs 129
Basic PKI 131
Smart Cards 132
Biometrics 133
Identity Technologies Summary 134

Host and Application Security 136
File System Integrity Checking 136
Host-Based Firewalls 137
HIDS 138
Host Antivirus 140
Host and Application Security Summary 142
Network Firewalls 142
Routers with Layer 3/4 Stateless ACLs 143
Stateful Firewalls 144
Network Firewalls Summary 146
Content Filtering 146
Proxy Servers 147
Web Filtering 148
E-Mail Filtering 150
Content-Filtering Summary 151
Network Intrusion Detection Systems 151
Signature-Based NIDS 152
Anomaly-Based NIDS 153
NIDS Summary 154
Cryptography 155
L2 Cryptography 156
Network Layer Cryptography 157
L5 to L7 Cryptography 158
File System Cryptography 159
Cryptography Summary 160
Emerging Security Technologies 161
Hybrid Host Solutions 161
Inline NIDS 162
Application Firewalls 162
Summary 162
References 165
Applied Knowledge Questions 165

Part II Designing Secure Networks 169

Chapter 5 Device Hardening 171

Components of a Hardening Strategy 171
Security Policy 172
Device Location 172
Threat Profile 172
Functional Requirements 172
Management Requirements 173

Network Devices 173
Router 174
Basic Hardening Settings 174
Authentication Settings 175
Management Access 178
Other Hardening Options 182
Switches 184
Firewalls 185
Login Restrictions 185
SSH 186
Logging 186
NIDS 186

Host Operating Systems 187
Partitioning Disk Space 188
Turning Off Unneeded Services 188
Patching the Services Needed 189
Logging Critical Events 189

Applications 189

Appliance-Based Network Services 190

Rogue Device Detection 191

Summary 192

References 192

Applied Knowledge Questions 193

Chapter 6 General Design Considerations 195

Physical Security Issues 195
Control Physical Access to Facilities 196
Lock-and-Key Access 196
Key Card Access 197
Key Card Access with Turnstile 197
Solving the Single-Factor Identity Problem 198
Control Physical Access to Data Centers 198
Separate Identity Mechanisms for Insecure Locations 199
Prevent Password Recovery Mechanisms in Insecure Locations 199
Be Aware of Cable Plant Issues 200
Be Aware of Electromagnetic Radiation 200
Be Aware of Physical PC Security Threats 201

Layer 2 Security Considerations 201
L2 Control Protocols 202
General Protocol Considerations 202
Cisco-Specific Protocols 205
MAC Flooding Considerations 210
Attack Details 211
Attack Mitigation 212
VLAN Hopping Considerations 213
Basic VLAN Hopping Attack 214
Creative VLAN Hopping Attacks 214
ARP Considerations 215
DHCP Considerations 218
DHCP Snooping 219
DHCP VACLs 220
Private VLANs 222
PVLAN Security Considerations 223
L2 Best Practices Recommendations 224

IP Addressing Design Considerations 224
General Best Practices and Route Summarization 224
Ingress/Egress Filtering 227
RFC 1918 227
RFC 2827 228
Nonroutable Networks 230
uRPF 232
NAT 233

ICMP Design Considerations 235
ICMP Rate Limiting 235
ICMP Message Type Filtering 235
ICMP Echo Request and ICMP Echo Reply 236
ICMP Destination Unreachable—Fragmentation Needed but DF Bit Set 238

HTTP/HTTPS 311
Simple Web Design 311
Two-Tier Web Design 311
Three-Tier Web Design 313

FTP 315
Active Mode 315
Passive Mode 316

Instant Messaging 316

Application Evaluation 317

Summary 318

References 319

Applied Knowledge Questions 319

Chapter 9 Identity Design Considerations 321

Basic Foundation Identity Concepts 321
Device Versus User Identity 322
Network Versus Application Identity 323
Whom Do You Trust? 323
Identity and Authentication, Authorization, and Accounting 324
Shared Identity 325
Cryptographic Identity Considerations 325

Types of Identity 326
Physical Access 326
MAC Addresses 327
IP Addresses 327
Layer 4 Information 327
Usernames 328
Digital Certificates 328
Biometrics 328

Factors in Identity 328

Role of Identity in Secure Networking 329

Identity Technology Guidelines 329
AAA Server Design Guidelines 330
Basic AAA Requirements 330
Remote User-Store Access 334
AAA Server Scalability 335
AAA Server Network Resiliency Considerations 336

Distributed AAA Server Synchronization Considerations 337
Distributed WAN Considerations 337
AAA Server Requirements 338
AAA Server Summary 338
802.1x/EAP Identity Design Guidelines 339
802.1x/EAP Protocol Details 339
802.1x/EAP Case Study 341
802.1x/EAP Design Considerations 342
802.1x/EAP Summary 346
Gateway-Based Network Authentication 346
PKI Usage Basics 347

Identity Deployment Recommendations 348
Device to Network 348
User to Network 348
User to Application 349

Summary 349

References 350

Applied Knowledge Questions 351

Chapter 10 IPsec VPN Design Considerations 353

VPN Basics 353

Types of IPsec VPNs 355
Site-to-Site VPNs 355
Remote User VPNs 356

IPsec Modes of Operation and Security Options 357
The Three Elements of IPsec 358
IKE 358
AH 358
ESP 359
Transport Mode and Tunnel Mode 360
IPsec SA Establishment 362
Phase 1 362
Phase 2: Quick Mode 363
Other Security Options 363
Authentication Methods 364
Diffie-Hellman Group 366
Perfect Forward Secrecy 366
Encryption Protocol Selection 367
Authentication/Integrity Protocol Selection 367

Topology Considerations 368
Split Tunneling 368
Performance 369
Security 370
Topology Choices 371
Hub and Spoke 371
Partial Mesh 372
Full Mesh 373
Distributed 374

Design Considerations 375
Platform Options 375
Site-to-Site IPsec Platforms 375
Remote User IPsec Platforms 376
Identity and IPsec Access Control 376
Layer 3 IPsec Considerations 376
Routing 377
NAT 377
GRE 378
IP Addressing 381
Fragmentation and Path Maximum Transmission Unit Discovery 381
Firewall and NIDS Placement for VPNs 384
Trusted IPsec Topology 385
Semitrusted IPsec Topology 386
High Availability 390
QoS 391
IPsec Vendor Interoperability 392

Site-to-Site Deployment Examples 392
Basic IPsec 393
GRE + IPsec 397
Basic GRE Hub and Spoke 397
HA GRE Hub and Spoke 402
GRE Design Conclusion 406
Dynamic Multipoint VPN 406
IPsec Outsourcing 407
Network-Based Managed IPsec 407
CPE Managed IPsec 408

Summary 408

References 408

Applied Knowledge Questions 409

Chapter 11 Supporting-Technology Design Considerations 413

Content 413
Caching 413
Security Considerations 414
Forward Proxy Cache 414
Transparent Cache 414
Reverse Proxy Cache 414
Content Distribution and Routing 415

Load Balancing 415
Security Considerations 416
Server Load Balancing 417
Security Considerations 417
SSL Offload 417
Security Device Placement 418
Security Device Load Balancing 419
When to Use 420
Deployment Options 421

Wireless LANs 424
General Considerations 425
Access Point Hardening 425
Rogue APs 425
Denial of Service 426
Physical Isolation Issues 427
Technology Options 427
802.11 WEP 427
802.11 Security Enhancements 429
L3+ Cryptography 431
WLAN Security Recommendations 438
Unique Deployment Options 438
Direct Internet Access WLAN 439
Differentiated Groups WLAN 440
WLAN Conclusion 441

IP Telephony 441
Security Considerations 442
Data Interception 442
DoS 443
Deployment Options 443
General Best Practices 444
IP Addressing/VLAN Separation 444
Firewalls 445
IP Telephony Recommendations 445

Summary 445

References 446

Applied Knowledge Questions 446

Chapter 12 Designing Your Security System 449

Network Design Refresher 449

Core, Distribution, Access/Edge 449

Management 454

Security System Concepts 455

Domains of Trust 455

Domains of Trust and Network Design 457

Domains of Trust Recommendations 460

Choke Points 460

Security Roles: Access/Edge, Distribution, Core 463

Impact of Network Security on the Entire Design 464

Routing and IP Addressing 464

Routing 464

IP Addressing 465

Manageability 466

Scalability and Performance 466

Ten Steps to Designing Your Security System 467

Step 1: Review Completed Security Policy Documents 468

Step 2: Analyze the Current Network Against the Security Policy 468

Step 3: Select Technologies and Evaluate Product Capabilities 469

Step 4: Design an Ideal Rough Draft of the Security System 470

Step 5: Test Key Components in a Lab 472

Step 6: Evaluate and Revise Design/Policy 472

Step 7: Finalize Design 472

Step 8: Implement the Security System in One Critical Area 472

Step 9: Roll Out to Other Areas 473

Step 10: Design/Policy Validation 473

Two-Step Evaluation Checklist 473

Evaluate Design for Policy Conformance 473

Evaluate Design for Threat Mitigation 473

Summary 475

Applied Knowledge Questions 475

Part III Secure Network Designs 479

Chapter 13 Edge Security Design 481

What Is the Edge? 481

Expected Threats 482

Threat Mitigation 485

Identity Considerations 485

Network Design Considerations 486

ISP Router 486

Number of Public Servers 487

Branch Versus Head-End Design Considerations 487

WAN Only 487

Internet VPN (No Services) 488

Internet (Limited Services) 488

Internet (Full Services) 488

Remote Access Alternatives 489

Small Network Edge Security Design 489

Design Requirements 490

Design Overview 490

Edge Devices and Security Roles 491

Router/Security Gateway 491

Optional WAN Router 492

Ethernet Switch 493

Public Servers 494

VPN 494

Site-to-Site 495

Remote User 495

Design Evaluation 496

VPN Evaluation 497

Design Alternatives 497

Outsourced Applications Alternative 497

Increased Security Alternative 497

Decreased Security Alternative 499

Medium Network Edge Security Design 500

Design Requirements 500

Design Overview 501

Internet Edge 502

Internet WAN Router 502

Stateful Firewall 502

NIDS 503

Ethernet Switch 503
Public Servers 504
Remote Access Edge 505
VPN 505
WAN 506
PSTN Dial-Up 506
Design Evaluation 507
Remote Access Design Evaluation 508
Design Alternatives 508
Increased VPN Requirements 509
Increased Security Alternative 510
Decreased Security Alternative 510

High-End Resilient Edge Security Design 512
Design Requirements 512
Design Overview 513
Multiple Public Server Segments 515
Routed Connections to the Campus 516
The Price of L2 Resiliency 516
Internet Edge 516
Internet WAN Router 517
Stateful Firewall 517
NIDS 518
Ethernet Switch 519
Public Servers 519
Remote Access Edge 520
VPN 521
WAN 522
PSTN Dial-Up 523
Design Evaluation 523
Remote Access Design Evaluation 524
Design Alternatives 525
Increased Security Alternative 525
Decreased Security Alternative 525

Provisions for E-Commerce and Extranet Design 526
E-Commerce 527
Extranet 528
General Extranet Design Considerations 529
Application-Based Extranets 529
Network-Based Extranets 530

Summary 531

References 531

Applied Knowledge Questions 531

hapter 14 Campus Security Design 535
What Is the Campus? 535
Campus Trust Model 536
Expected Threats 536
Threat Mitigation 539
Identity Considerations 540
Network Design Considerations 541
Layer 2 Considerations 541
Stateful Versus Stateless ACLs and L3 Versus L4 Filtering 541
Intrusion Detection Systems 541
WLAN Considerations 542
Network Management 542
Rogue Devices 542
Small Network Campus Security Design 543
Design Requirements 543
Design Overview 543
Campus Devices and Security Roles 544
Ethernet Switch 544
Internal Servers 545
User Hosts 545
WLAN AP 546
Optional AAA Server 546
Design Evaluation 546
Design Alternatives 547
Increased Security Alternative 548
Decreased Security Alternative 548
Medium Network Campus Security Design 549
Design Requirements 549
Design Overview 549
Campus Devices and Security Roles 550
Ethernet Switches (All) 550
Ethernet Switches (L3 Distribution/Core) 551
Internal Servers 551
User Hosts 552
NIDS 553
AAA Server 553
WLAN AP 553

Design Evaluation 554
Design Alternatives 555
Increased Security Alternative 555
Decreased Security Alternative 556

High-End Resilient Campus Security Design 557
Design Requirements 557
Design Overview 557
Campus Devices and Security Roles 559
Ethernet Switches (All) 560
Ethernet Switches (User) 560
Ethernet Switches (L3 Distribution) 560
Ethernet Switches (Data Center) 561
Ethernet Switches (Core) 561
Internal Servers 562
User Hosts 562
NIDS 563
Stateful Firewalls 563
AAA Server 564
Certificate Authority 564
WLAN AP 565
Design Evaluation 565
Design Alternatives 566
Increased Security Alternative 566
Decreased Security Alternative 567

Summary 567

References 567

Applied Knowledge Questions 567

Chapter 15 Teleworker Security Design 571

Defining the Teleworker Environment 571

Expected Threats 572

Threat Mitigation 575

Identity Considerations 575

Network Design Considerations 576
Host Protections 576
Network-Transit Protections 577

Software-Based Teleworker Design 578
Design Requirements 578
Design Overview 578

Hardware-Based Teleworker Design 579
Design Requirements 580
Design Overview 580
Physical Security Considerations 583

Design Evaluations 583

Summary 585

Reference 585

Applied Knowledge Questions 585

rt IV Network Management, Case Studies, and Conclusions 589

hapter 16 Secure Network Management and Network Security Management 591

Utopian Management Goals 591

Organizational Realities 593

Protocol Capabilities 594
Telnet/Secure Shell 594
Typical Use 594
Security Considerations 595
Deployment Best Practices 595
HTTP/HTTPS 596
Typical Use 596
Security Considerations 596
Deployment Best Practices 596
Simple Network Management Protocol 596
Typical Use 597
Security Considerations 597
Deployment Best Practices 598
TFTP/FTP/SFTP/SCP 599
Typical Use 599
Security Considerations 600
Deployment Best Practices 600
Syslog 601
Typical Use 601
Security Considerations 601
Deployment Best Practices 602

NetFlow 602
Typical Use 603
Security Considerations 604
Deployment Best Practices 604
Others 605

Tool Capabilities 605
Network Security Management Tools 606
Configuration/Provisioning Tools 606
Security Monitoring Tools 607
Secure Network Management Tools 608

Secure Management Design Options 608
Cleartext In-Band 608
Supported Platforms 609
Multisite Considerations 609
Attack Mitigation 609
Best Deployment Practices 610
Cryptographically Secure In-Band (Session and Application Layer) 611
Supported Platforms 611
Multisite Considerations 611
Attack Mitigation 611
Best Deployment Practices 611
Cryptographically Secure In-Band (Network Layer) 612
Supported Platforms 613
Multisite Considerations 614
Attack Mitigation 615
Best Deployment Practices 615
Out of Band (OOB) 616
Supported Platforms 619
Multisite Considerations 619
Threats and Attack Mitigation 620
Best Deployment Uses 621
Hybrid Management Design 622
Secure Network Management Optional Components 623

Network Security Management Best Practices 625
Monitor Critical Security Events 24*7*365 625
Separate Historical Event Data from Critical Notifications 626
Choose Sensible Logging Levels 626
Separate Network Management and Network Security Management 627
Focus on Operational Requirements 628
Consider Outsourcing 629

Summary 630

References 631

Applied Knowledge Questions 632

hapter 17 Case Studies 635

Introduction 635

Real-World Applicability 635

Organization 635

Organization Overview 636
Current Design 636
Security Requirements 636
Design Choices 636
Migration Strategy 636
Attack Example 637

NetGamesRUs.com 637

Organization Overview 637
Current Design 637
Security Requirements 638
Campus Security 638
Edge Security 639
Management 639
Design Choices 640
Migration Strategy 642
Attack Example 643

University of Insecurity 643

Organization Overview 643
Current Design 643
Security Requirements 644
Internet Connectivity 645
Student Connectivity 645
Administrative Systems 645
Management Systems 645
WAN Connected Networks 645
Design Choices 646
Basic Changes 647
Internet Connectivity 647
Student Networks 648
Administrative Networks 648
Management Network 648
Migration Strategy 649
Attack Example 649
DDoS Infections/Attacks 649
Critical System Compromises 650
Student Network Attacks 650

Black Helicopter Research Limited 650
Organization Overview 651
Current Design 651
Security Requirements 652
Internet Connectivity 653
Classified Network 653
WAN Connectivity 653
User Education 653
Design Choices 654
Physical Security 654
Network Security System 656
Migration Strategy 658
Attack Example 659

Summary 659

Reference 660

Applied Knowledge Questions 660

Chapter 18 Conclusions 663

Introduction 663

Management Problems Will Continue 663

Security Will Become Computationally Less Expensive 665

Homogeneous and Heterogeneous Networks 665

Legislation Should Garner Serious Consideration 666

IP Version 6 Changes Things 668

Network Security Is a System 669

Summary 670

References 670