Contents

Foreword xxxi

Chapter 1 DMZ Concepts, Layout, and Conceptual Design 1

Introduction 2
Planning Network Security 2
Security Fundamentals 3
Identifying Risks to Data 6
Identifying Risks to Services 7
Identifying Potential Threats 8
Introducing Common Security Standards 9
Policies, Plans, and Procedures 10
DMZ Definitions and History 12
DMZ Concepts 13
Traffic Flow Concepts 17
Networks With and Without DMZs 21
Pros and Cons of DMZ Basic Designs 22
DMZ Design Fundamentals 24
Why Design Is So Important 25
Designing End-to-End Security for Data Transmission Between Hosts on the Network 25
Traffic Flow and Protocol Fundamentals 26
DMZ Protocols 26
Designing for Protection in Relation to the Inherent Flaws of TCP/IPv4 27
Public and Private IP Addressing 28
Ports 29
The OSI Model 30
Identifying Potential Risks from the Internet 31
Using Firewalls to Protect Network Resources 32

Using Screened Subnets to Protect Network Resources 32
Securing Public Access to a Screened Subnet 33
Traffic and Security Risks 35
Application Servers in the DMZ 35
Domain Controllers in the DMZ 36
RADIUS-Based Authentication Servers in the DMZ 36
VPN DMZ Design Concepts 36
Advanced Risks 37
Business Partner Connections 37
Extranets 38
Web and FTP Sites 38
E-Commerce Services 39
E-Mail Services 39
Advanced Design Strategies 39
Advanced DMZ Design Concepts 40
Remote Administration Concepts 41
Authentication Design 43
Summary 44
Solutions Fast Track 45
Frequently Asked Questions 47

Chapter 2 Windows 2000 DMZ Design 49
Introduction 50
Introducing Windows 2000 DMZ Security 51
Fundamental Windows 2000 DMZ Design 52
Network Engineering the DMZ 54
Systems-Engineering the DMZ 60
Security Analysis for the DMZ 62
Building a Windows 2000 DMZ 63
Designing the DMZ Windows Style 64
Domain Considerations 64
The Contained Domain Model 66
The Extended Domain Model 67
The Internet Connection 67
Wide Area Network Link 69
DMZ Perimeter Security 75
External Router 75

Firewall 75
Extra DMZ Routers 78
Name Resolution for the DMZ 79
DMZ Mail Services 80
Mail Relay 81
Web Servers 82
External Web Server 82
Designing Windows 2000 DNS in the DMZ 83
External DNS Server 84
Engineering Windows 2000 Traffic in the DMZ 85
Assessing Network Data Visibility Risks 89
Windows 2000 DMZ Design Planning List 92
Summary 94
Solutions Fast Track 95
Frequently Asked Questions 100

Chapter 3 Sun Solaris DMZ Design 103

Introduction 104
Placement of Servers 104
The Firewall Ruleset 108
The Private Network Rules 108
The Public Network Rules 111
Server Rules 113
System Design 114
Hardware Selection: The Foundation 116
Common DMZ Hardware Requirements 117
Network Hardware Considerations 117
Software Selection: The Structure 118
Popular Firewall Software Packages 119
High Availability of the DMZ Server 120
Host Security Software 121
Other Software Considerations 122
Configuration: The Plumbing and Other Details 123
Disk Layout and Considerations 123
Increasing the Verbosity of Local Auditing 124
Backup Considerations 125
Remote Administration 126

Putting the Puzzle Together 126
Layering Local Security 128
Auditing Local File Permissions 130
Building the Model for Future Use 133
Implementation: The Quick, Dirty Details 135
Media Integrity 135
Physical Host Security 135
Host Network Security 136
Patch Application 136
Solaris System Hardening 137
Manual System Hardening 138
Automated System Hardening 143
Hardening Checklists for DMZ Servers and Solaris 145
Summary 147
Solutions Fast Track 148
Frequently Asked Questions 150

Chapter 4 Wireless DMZs 153

Introduction 154
Why Do We Need Wireless DMZs? 156
Passive Attacks on Wireless Networks 156
War Driving 157
Sniffing 160
Active Attacks on Wireless Networks 160
Spoofing (Interception) and Unauthorized Access 161
Denial of Service and Flooding Attacks 164
Man-in-the-Middle Attacks on Wireless Networks 166
Network Hijacking and Modification 166
Jamming Attacks 168
Designing the Wireless DMZ 169
Wireless DMZ Components 171
Access Points 172
Network Adapters 172
RADIUS Servers 173
Enterprise Wireless Gateways and Wireless Gateways 173
Firewalls and Screening Routers 174
Other Segmentation Devices 174

Wireless DMZ Examples 174
Wireless LAN Security Best-Practices Checklist 178
Summary 181
Solutions Fast Track 181
Frequently Asked Questions 183

Chapter 5 Firewall Design: Cisco PIX 185

Introduction 186
Basics of the PIX 186
Securing Your Network Perimeters 187
The Cisco Perimeter Security Solution 187
Cisco PIX Versions and Features 192
Cisco PIX Firewalls 192
The Cisco PIX 501 Firewall 192
The Cisco PIX 506E Firewall 193
The Cisco PIX 515E Firewall 194
The Cisco PIX 525 Firewall 196
The Cisco PIX 535 Firewall 197
Cisco Firewall Software 198
The Cisco PIX Device Manager 199
Cisco PIX Firewall Licensing 200
Cisco PIX Firewall Version 6.3 201
PIX Firewall PCI Card Options 202
Making a DMZ and Controlling Traffic 207
Securely Managing the PIX 207
The Console 207
Telnet 208
SSH 209
The PIX Device Manager 210
Authenticating Management Access to the PIX 212
PIX Configuration Basics 213
Defining Interfaces 213
Configuring NAT 218
Outbound NAT 220
Inbound NAT 225
Verifying and Monitoring NAT 229
Configuring Access Rules 229
Creating an Outbound Access Control List 230

Creating an Inbound Access Control List 232
Creating Turbo ACLs 232
Monitoring ACLs 233
Routing Through the PIX 235
Static Routing 235
Enabling RIP 237
OSPF 238
Configuring Advanced PIX Features 239
The PIX Failover Services 239
What Causes Failover to Occur 240
Failover Requirements 240
Configuring Stateful Failover with a Failover Cable 241
Configuring Stateful LAN-Based Failover 244
Testing and Monitoring Failover 247
Blocking ActiveX and Java 247
URL Filtering 248
Cut-Through Proxy 249
Application Inspection 250
Intrusion Detection 251
FloodGuard, FragGuard, and DNSGuard 251
Securing SNMP and NTP 252
PIX Firewall Design and Configuration Checklist 253
Summary 254
Solutions Fast Track 255
Frequently Asked Questions 257

Chapter 6 Firewall and DMZ Design: Check Point NG 259

Introduction 260
Basics of Check Point NG 260
Stateful Inspection 261
Network Address Translation 261
Management Architecture 262
Securing Your Network Perimeters 262
The Check Point Perimeter Security Solution 262
Configuring Check Point to Secure Network Perimeters 263
Antispoofing 264

SmartDefense 266
Stateful Inspection Customization 273
Making a DMZ and Controlling Traffic 275
Configuring the DMZ Interface 275
Configuring Access Rules 277
Configuring Network Address Translation 279
Routing Through Check Point FireWall-1/VPN-1 280
Check Point NG Secure DMZ Checklist 280
Summary 282
Solutions Fast Track 282
Frequently Asked Questions 283

Chapter 7 Firewall and DMZ Design: Nokia Firewall 285

Introduction 286
Basics of the Nokia Firewall 286
Choosing the Right Platform 287
Nokia IP120 Appliance 287
Nokia IP350/IP380 Platforms 287
Nokia IP530 Platform 288
Nokia IP710/IP740 Platform 289
Configuring the Nokia Appliance 290
Serial Console Access 290
Configuring IPSO Settings 291
Using CLISH 292
Software Installation 294
Securing Your Network Perimeters 296
Plan Ahead 296
Know the Purpose of Your DMZ 297
DMZ Type 297
New or Existing Network 297
Network Plan 297
Time Constraints 298
Available Support Assistance 298
The Nokia Perimeter Security Solution 299
Configuring Check Point FireWall-1 Address Translation Rules 299
Building the DMZ 304

Configuring Check Point FireWall-1 Security and Address Translation Rules 310
Additional Considerations for Designing a DMZ 311
Nokia Firewall and DMZ Design Checklist 315
Summary 316
Solutions Fast Track 316
Frequently Asked Questions 319

Chapter 8 Firewall and DMZ Design: ISA Server 2000 321

Introduction 322
Configuring a Trihomed DMZ 322
The Network Layout 324
CLIENTDC 325
ISA 326
Internal Interface 326
External Interface 326
DMZ Interface 326
DMZSMTPRELAY 326
Router 327
Interface #1 (the DMZ Interface) 327
Interface #2 (the Public Interface) 327
Laptop (External Network Client) 327
Configuring the ISA Server 328
Ping Testing the Connections 330
Creating an Inbound ICMP Ping Query Packet Filter on the ISA Server External Interface 331
Creating an Inbound ICMP Ping Query Packet Filter to the DMZ Host's Interface 334
Pinging the ISA Server Interfaces from the DMZ Hosts 337
Creating a Global ICMP Packet Filter for DMZ Hosts 337
Publishing DMZ SMTP Servers 338
Publishing a DMZ SMTP Mail Relay Server 342
Publishing a Web Server 350
Publishing an FTP Server on a Trihomed DMZ Segment 351
How FTP Works 351
Normal or PORT or Active Mode FTP 351
Passive or PASV Mode FTP 352

Challenges Created by the FTP Protocol 353
PORT Mode FTP Client-Side Firewall 354
PORT Mode FTP Server-Side Firewall 354
PASV Mode FTP Client-Side Firewall 355
PASV Mode FTP Client-Side Firewall 356
Using Packet Filters to Publish the PORT Mode FTP Server 356
Using Packet Filters to Publish the PASV Mode FTP Server 359
Beware the "Allow All" Packet Filter 360
External Network Clients Cannot Use the DMZ Interface to Connect to the Internal Network 362
Summary 364
Solutions Fast Track 364
Frequently Asked Questions 366

Chapter 9 DMZ Router and Switch Security 369

Introduction 370
Securing the Router 370
Router Placement in a DMZ Environment 370
Border Gateway Protocol 375
Access Control Lists 379
Security Banner 385
Securely Administering the Router 386
Disabling Unneeded IOS features 397
Cisco Discovery Protocol 398
Redirects 398
Unreachables 399
Directed Broadcasts 399
Proxy ARP 400
Small Services 400
Finger 401
IP Source Routing 401
Bootp Server 402
Other Security Features 402
Securing the Switch 403
Cisco Switches 404
Catalyst 2950 404

Catalyst 3550 405
Catalyst 4500 405
Catalyst 6500 406
Securely Managing Switches 407
Console 408
Telnet 408
SSH 410
HTTP 410
Enable Passwords 410
AAA 411
Syslogs, SNMP, and NTP 412
Security Banner 412
Disabling Unneeded IOS features 412
VLAN Trunking Protocol 413
VLANs 414
Private VLANS 419
Securing Switch Ports 422
IOS Bugs and Security Advisories 424
DMZ Router and Switch Security Best-Practice Checklists 425
Router Security Checklist 425
Switch Security Checklist 426
Summary 428
Solutions Fast Track 428
Frequently Asked Questions 430

Chapter 10 DMZ-Based VPN Services 433

Introduction 434
VPN Services in the DMZ 434
VPN Deployment Models 435
VPN Termination at the Edge Router 436
VPN Termination at the Corporate Firewall 438
VPN Termination at a Dedicated VPN Appliance 439
Topology Models 440
Meshed Topology 440
Star Topology 441
Hub-and-Spoke Topology 442
Remote Access Topology 442

Placement of Devices 443
Business Partner Connections 444
Remote Access Services 444
Nokia 445
NetScreen VPNs 446
Cisco VPNs 447
Windows VPN 450
Designing an IPSec Solution 451
Designing an IPSec Encryption Scheme 451
Designing an IPSec Management Strategy 452
Designing Negotiation Policies 453
Designing Security Policies 453
Designing IP Filters 454
Defining Security Levels 454
Connecting B2B Sites 455
Extranets 455
VPN Security 456
Active Directory Security 457
Summary 459
Solutions Fast Track 459
Frequently Asked Questions 461

Chapter 11 Implementing Wireless DMZs 463

Introduction 464
Implementing a Wireless Gateway with Reef Edge Dolphin 464
Installing Dolphin 467
Configuring Dolphin 472
Improving the User Experience 475
Dolphin Review 477
Implementing RADIUS with Cisco LEAP 477
LEAP Features 478
Building a LEAP Solution 480
Installing and Configuring Steel Belted Radius 482
Configuring LEAP 486
Windows Active Directory Domain Authentication with LEAP and RADIUS 491
LEAP Review 493

Summary 495
Solutions Fast Track 495
Frequently Asked Questions 496

Chapter 12 Sun Solaris Bastion Hosts 499
Introduction 500
Configuring the Fundamentals 500
System Installation 501
Minimizing Services 502
Additional Steps 505
System Patching 507
Removing SUID Programs 507
TCP/IP Stack Hardening 508
Controlling Access to Resources 509
Address-Based Access Control 510
Configuring TCP Wrappers 510
Cryptographic Access Control 513
Creating an IPSec Policy File 514
Auditing Access to Resources 517
The SunScreen Basic Security Module 518
BSM Configuration 518
Viewing Audit Data 520
Authentication 521
Bastion Host Configuration 523
SMTP Relays 524
FTP and Web Servers 528
Sun Solaris Bastion Hosts Checklists 529
Summary 531
Solutions Fast Track 531
Frequently Asked Questions 533

Chapter 13 Windows 2000 Bastion Hosts 535
Introduction 536
Configuring the Fundamentals 536
Domain Members or Standalone Servers? 537
Installing from Scratch 538
Disk Partitions 538
Removing Optional Components 539

Service Packs and Hotfixes 539
Creating a New Local Administrator 542
Security Configuration Through the Microsoft Management Console 542
Account Lockout Policy (Under Account Policies) 544
Audit Policy (Under Local Policies) 544
User Rights Assignment (Under Local Policies) 546
Security Options (Under Local Policies) 547
Event Log 549
Restricted Groups 549
System Services 550
Registry and File System ACLs 551
Applying the High-Security DMZ Template 555
Remote Administration of DMZ Hosts 556
Using Terminal Services for Remote Desktop Administration 556
Installing Terminal Services 558
Configuring Terminal Services Securely 558
Using Terminal Services for File Replication 561
Using IPSec-Enhanced Telnet for Command-Line Administration 562
Vulnerability-Scan Your Host 565
Bastion Host Configuration 567
Configuring IIS Servers for Web Access 567
Setting Up an Anonymous, Public Web Site 567
The IIS Lockdown Tool 570
The URLScan Tool (New and Improved) 576
Final Configuration Steps 577
Setting Up a Secure Web Site 579
Configuring an IIS Server for FTP 581
Configuring an IIS Server for SMTP 582
Checklists 583
Windows 2000 Server Hardening Checklist 583
IIS Hardening Checklist (WWW, FTP, and SMTP) 584
For World Wide Web Service (HTTP) 584
For World Wide Web Service (HTTPS) 586

For FTP Service 586
For SMTP Service 586
Summary 587
Solutions Fast Track 587
Frequently Asked Questions 589
Checklists 590

Chapter 14 Hacking the DMZ 593

Introduction 594
Reconnaissance and Penetration Testing 597
Defense in Depth 597
Recon 101 600
Picking a Target 602
Basic Information Gathering 603
Whois Lookup 605
Social Engineering 610
Hiding Your Identity 611
Scanning Techniques 613
Network Mapping 616
Vulnerability Scanning 626
Auditing and Logging Evasion 632
Probing Analog Connections 632
Attacking the DMZ Hosts 638
DNS Exploits 638
General BIND Security 644
DNS Spoofing Attacks 645
SQL Attacks and Hacks 647
E-Mail Attacks and Hacks 651
Other Attack Methods 655
DMZ Hardening Checklist 657
Summary 659
Solutions Fast Track 660
Frequently Asked Questions 663

Chapter 15 Intrusion Detection in the DMZ 667
Introduction 668
Intrusion Detection 101 672
Deployment of an IDS 678
Repelling the Hacker 685
Honeypots in the DMZ 687
Configuring a Honeypot for Your DMZ 687
Host-Based Intrusion Detection Systems 689
Tripwire 690
Saving the DNS Server 692
Implementing HIDS on Your DNS Server 694
Keeping the Web Server Serving 695
CiscoSecure IDS 697
Snort 706
The Poor Man's IDS 714
Network Time 717
More IDS Deployment Strategies 717
Case Study 720
Lessons Learned 721
Summary 722
Solutions Fast Track 723
Frequently Asked Questions 725
Index 727