

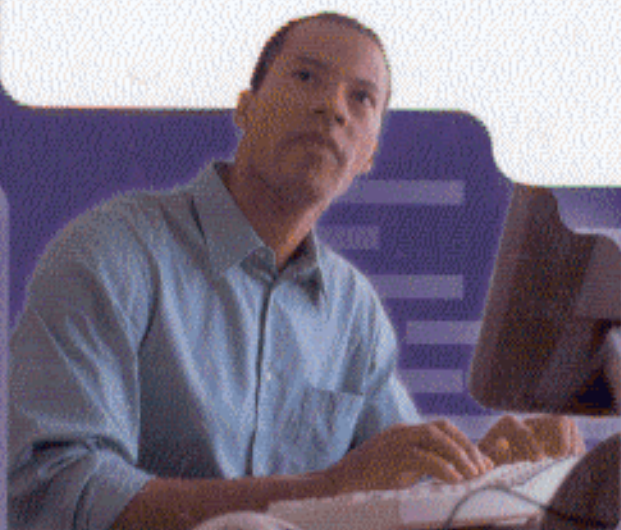
Microsoft

MCSE

**Exam
70-220**

Designing Microsoft Windows 2000 Network Security

Training Kit



CD Includes
120-day evaluation
version of
Microsoft
**Windows 2000
Advanced
Server**

- ▶ Official Microsoft study guide for MCP Exam 70-220: *Designing Security for a Microsoft Windows 2000 Network*
- ▶ Work at your own pace and practice your design skills in challenging case studies
- ▶ Develop real-world expertise by mastering the concepts, principles, and tasks measured by certification exam objectives

IT Professional

Contents

About This Book	xxix
Intended Audience	xxx
Prerequisites	xxx
Reference Materials	xxxi
About the Supplemental Course Materials CD-ROM	xxxi
Features of This Book	xxxii
Notes	xxxii
Conventions	xxxii
Chapter and Appendix Overview	xxxiii
Finding the Best Starting Point for You	xxxvi
Where to Find Specific Skills in This Book	xxxvi
Getting Started	xl
Hardware Requirements	xl
Software Requirements	xl
Setup Instructions	xli
About the Online Book	xlvi
Sample Readiness Review Questions	xlvi
The Microsoft Certified Professional Program	xlix
Microsoft Certification Benefits	xlix
Requirements for Becoming a Microsoft Certified Professional	li
Technical Training for Computer Professionals	lii
Technical Support	liv
 Chapter 1 Introduction to Microsoft Windows 2000 Security	1
About This Chapter	1
Before You Begin	1
Chapter Scenario: Lucerne Publishing	2
Current Network	2
Account Management	2
Expansion Plans	3
Online Ordering	3
Security Issues	3
Lesson 1: Microsoft Windows 2000 Security Services Overview	4
Security Subsystem Components	5
LSA Functionality	7

Windows 2000 Security Protocols	8
The Security Support Provider Interface (SSPI)	9
Lesson Summary	9
Lesson 2: Designing Security Business Requirements	10
Determining Business Requirements	10
Making the Decision	12
Applying the Decision	13
Lesson Summary	14
Lesson 3: Designing Security to Meet Technical Requirements	15
Determining Technical Requirements	15
Making the Decision	16
Applying the Decision	17
Lesson Summary	19
Review	20
 Chapter 2 Designing Active Directory for Security	21
About This Chapter	21
Before You Begin	22
Chapter Scenario: Wide World Importers	23
The Existing Network	23
User Account Management	23
Application Support	23
Client Desktops	24
Lesson 1: Designing Your Forest Structure	25
Active Directory Design Basics	25
Deploying a Single Forest	26
Making the Decision	27
Applying the Decision	28
Deploying Multiple Forests	28
Making the Decision	30
Applying the Decision	31
Lesson Summary	32
Lesson 2: Designing Your Domain Structure	33
Deploying a Single Domain	33
Making the Decision	33
Applying the Decision	34
Deploying Multiple Domains	34
Understanding Account Policies	34
Making the Decision	37

Applying the Decision	38
Lesson Summary	39
Lesson 3: Designing an OU Structure	40
Planning for Delegation of Administration	40
Delegating Control to an Organizational Unit	40
Making the Decision	42
Applying the Decision	44
Planning for Group Policy Deployment	45
Making the Decision	49
Applying the Decision	49
Lesson Summary	51
Lesson 4: Designing an Audit Strategy	52
Configuring Audit Settings	52
Making the Decision	53
Applying the Decision	54
Lesson Summary	55
Activity: Designing an Audit Strategy	56
Lab 2-1: Designing Active Directory for Security	57
Lab Objectives	57
About This Lab	57
Before You Begin	57
Scenario: Contoso Ltd.	57
Exercise 1: Determining the Number of Forests	59
Exercise 2: Determining the Number of Domains	60
Exercise 3: Designing an OU Structure	60
Review	62
 Chapter 3 Designing Authentication for a Microsoft Windows 2000 Network	63
About This Chapter	63
Before You Begin	64
Chapter Scenario: Market Florist	65
The Existing Network	65
Market Florist Active Directory Design	66
Market Florist Server Configuration	66
Lesson 1: Designing Authentication in a Microsoft Windows 2000 Network ..	68
Determining Business and Technical Requirements	68
Lesson Summary	69
Lesson 2: Designing Kerberos Authentication	70
Designing Kerberos Authentication	71

Understanding the Kerberos Message Exchanges	72
Analyzing Kerberos Authentication	73
Initial Authentication with the Network	73
Network Authentication	76
Smart Card Authentication	77
Multiple Domain Authentication	79
Delegation	80
Making the Decision	82
Applying the Decision	83
Lesson Summary	84
Lesson 3: NTLM Authentication	85
Designing NTML Authentication	85
Making the Decision	86
Applying the Decision	87
Lesson Summary	87
Lesson 4: Authenticating Down-Level Clients	88
Analyzing Standard Authentication	88
Analyzing the Directory Services Client	89
Making the Decision	92
Applying the Decision	92
Lesson Summary	93
Lesson 5: Planning Server Placement for Authentication	94
Determining Server Placement for Authentication	94
Planning DNS Server Placement	94
Making the Decision	95
Applying the Decision	95
Planning DC Placement	97
Making the Decision	97
Applying the Decision	97
Planning Global Catalog Server Placement	97
Making the Decision	98
Applying the Decision	99
Planning PDC Emulator Placement	99
Making the Decision	99
Applying the Decision	100
Lesson Summary	100
Activity: Analyzing Authentication Network Infrastructure	101
Lab 3-1: Designing Authentication for the Network	102
Lab Objectives	102

About This Lab	102
Before You Begin	102
Scenario: Contoso Ltd.	102
Exercise 1: Designing Windows 2000 Client Authentication	104
Exercise 2: Designing Down-Level Client Authentication	105
Review	106
 Chapter 4 Planning a Microsoft Windows 2000 Administrative Structure	107
About This Chapter	107
Before You Begin	107
Chapter Scenario: Hanson Brothers	108
The Existing Network	108
Hanson Brothers' Active Directory Design	109
Hanson Brothers' Administrative Needs	109
The Central Administration Team	110
Hanson Brothers' Current Issues	110
Lesson 1: Planning Administrative Group Membership	111
Designing Default Administrative Group Membership	111
The Default Windows 2000 Administrative Groups	111
Assessing Administrative Group Membership Design	114
Making the Decision	116
Applying the Decision	117
Designing Custom Administrative Groups	118
Determining When to Create Custom Groups	119
Making the Decision	120
Applying the Decision	121
Lesson Summary	122
Lesson 2: Securing Administrative Access to the Network	123
Designing Secure Administrative Access	123
Making the Decision	124
Applying the Decision	125
Designing Secondary Access	126
Understanding the RunAs Service	127
Making the Decision	129
Applying the Decision	129
Designing Telnet Administration	129
Making the Decision	130
Applying the Decision	130
Designing Terminal Services Administration	131

Assessing Terminal Services Administration	131
Making the Decision	132
Applying the Decision	132
Lesson Summary	133
Activity: Administering the Network	134
Lab 4-1: Designing Administration for a Microsoft Windows 2000 Network	136
Lab Objectives	136
About This Lab	136
Before You Begin	136
Scenario: Contoso Ltd.	136
Exercise 1: Designing Preexisting Administration Groups	138
Exercise 2: Designing Administrative Access	140
Review	142
Chapter 5 Designing Group Security	143
About This Chapter	143
Before You Begin	143
Chapter Scenario: Hanson Brothers	144
The Microsoft Exchange 2000 Server Deployment	144
Deployment of Microsoft Outlook 2000	144
User Rights Requirements	145
Lesson 1: Designing Microsoft Windows 2000 Security Groups	146
Windows 2000 Groups	146
Assessing Group Usage	149
Making the Decision	152
Applying the Decision	152
Lesson Summary	154
Activity: Reviewing Group Memberships	155
Lesson 2: Designing User Rights	158
Defining User Rights with Group Policy	158
User Rights Within Windows 2000	158
Assessing Where to Apply User Rights	162
Making the Decision	163
Applying the Decision	164
Lesson Summary	165
Lab 5-1: Designing Security Groups and User Rights	166
Lab Objectives	166
About This Lab	166

Before You Begin	166
Scenario: Contoso Ltd.	166
The Human Resources Application	166
Exercise 1: Designing Security Groups	168
Exercise 2: Designing User Rights	170
Review	171
Chapter 6 Securing File Resources	173
About This Chapter	173
Before You Begin	173
Chapter Scenario: Wide World Importers	174
Planning Security for Software Deployment	174
Print Security	176
Planning for Protection of Confidential Data	176
Lesson 1: Securing Access to File Resources	177
Designing Share Security	177
Configuring Share Permissions	177
Making the Decision	179
Applying the Decision	180
Planning NTFS Security	180
Changes in the Windows 2000 NTFS File System	181
Assessing NTFS Permissions	181
Making the Decision	183
Applying the Decision	184
Combining Share and NTFS Security	185
Making the Decision	187
Applying the Decision	188
Lesson Summary	188
Activity: Evaluating Permissions	189
Lesson 2: Securing Access to Print Resources	191
Assessing Printer Security	191
Making the Decision	192
Applying the Decision	193
Lesson Summary	193
Lesson 3: Planning EFS Security	194
Overview of the EFS Process	194
Designating an EFS Recovery Agent	197
The Initial EFS Recovery Agent	197
Configuring a Custom EFS Recovery Agent	198

Configuring an Empty Encrypted Data Recovery Agent Policy	199
Making the Decision	199
Applying the Decision	200
Recovering Encrypted Files	200
Assessing Recovery of Encrypted Files	200
Making the Decision	202
Applying the Decision	202
Lesson Summary	202
Lab 6-1: Securing File and Print Resources	203
Lab Objectives	203
About This Lab	203
Before You Begin	203
Scenario: Contoso Ltd.	203
Exercise 1: Planning File Security	206
Exercise 2: Planning Print Security	207
Exercise 3: Planning EFS for Laptops	208
Review	210
Chapter 7 Designing Group Policy	211
About This Chapter	211
Before You Begin	211
Chapter Scenario: Wide World Importers	212
Proposed OU Structure	212
Existing Site Definitions	213
Application Installation Requirements	213
Engineering Requirements	213
The New Employee	214
Lesson 1: Planning Deployment of Group Policy	215
Group Policy Overview	215
Planning Group Policy Inheritance	215
Assessing Group Policy Application	217
Block Policy Inheritance	218
Configuring No Override	219
Making the Decision	219
Applying the Decision	220
Filtering Group Policy by Using Security Groups	221
Making the Decision	223
Applying the Decision	224
Lesson Summary	224

Lesson 2: Troubleshooting Group Policy	225
Assessing Group Policy Troubleshooting	225
Making the Decision	227
Applying the Decision	228
Lesson Summary	228
Activity: Troubleshooting Group Policy Application	229
Lab 7-1: Planning Group Policy Deployment	230
Lab Objectives	230
About This Lab	230
Before You Begin	230
Scenario: Contoso Ltd.	230
Exercise 1: Applying Group Policy	233
Exercise 2: Designing Group Policy Filtering	233
Exercise 3: Troubleshooting Group Policy Application	234
Review	237
 Chapter 8 Securing Microsoft Windows 2000-Based Computers	239
About This Chapter	239
Before You Begin	239
Chapter Scenario: Market Florist	240
Market Florist Domain Structure	240
Market Florist Computers	240
Computer Roles	240
Security Requirements	242
The Flower Power Application	242
Security Requirements for the Internal Network	242
Lesson 1: Planning Microsoft Windows 2000 Security Templates	243
Introducing Windows 2000 Security Templates	243
Determining Common Security Requirements	245
Making the Decision	246
Applying the Decision	246
Analyzing Default Security in Windows 2000	247
Securing Newly Installed Computers	248
Securing Upgraded Computers	248
Making the Decision	249
Applying the Decision	249
Using Incremental Security Templates	250
Making the Decision	254
Applying the Decision	255

Creating Custom Security Templates	255
Making the Decision	255
Applying the Decision	256
Extending the Security Configuration Tool Set	256
The Sceregvl.inf File	257
Making the Decision	259
Applying the Decision	259
Lesson Summary	260
Activity: Evaluating a Security Template	261
Lesson 2: Analyzing Security Settings with Security Configuration and Analysis	263
Comparing Security Settings to the Security Template	263
Performing the Analysis	263
Making the Decision	266
Applying the Decision	267
Lesson Summary	268
Lesson 3: Planning the Deployment of Security by Using Security Templates	269
Deploying Security Templates in a Workgroup	269
Making the Decision	270
Applying the Decision	270
Deploying Security Templates in a Windows 2000 Domain	271
Making the Decision	272
Applying the Decision	273
Lesson Summary	274
Lab 8-1: Planning Security Templates	275
Lab Objectives	275
About This Lab	275
Before You Begin	275
Scenario: Contoso Ltd.	275
Exercise 1: Determining Computer Classifications	279
Exercise 2: Developing Custom Security Templates	280
Exercise 3: Planning Deployment of the Security Templates	282
Review	283
Chapter 9 Designing Microsoft Windows 2000 Services Security	285
About This Chapter	285
Before You Begin	286
Chapter Scenario: Lucerne Publishing	287
Active Directory Design for Lucerne Publishing	287

Lucerne Publishing's Active Directory	287
DNS Services	287
DHCP Services	288
Remote Installation Services (RIS)	288
Simple Network Management Protocol (SNMP)	289
Terminal Services	289
Lesson 1: Designing DNS Security	290
Assessing Security Risks for the DNS Service	290
Securing Dynamic Updates	291
Restricting Zone Transfers	292
Implementing Separate External DNS Servers	293
Restricting Membership in the DNS Admins Group	293
Making the Decision	293
Applying the Decision	294
Lesson Summary	294
Activity: Designing DNS for Internal and External Use	295
Lesson 2: Designing DHCP Security	297
Assessing the Security Risks of the DHCP Service	297
Preventing Unauthorized DHCP Servers	297
Preventing DHCP Servers from Overwriting Static IP Addresses in DNS	298
Preventing Unauthorized DHCP Clients from Leasing IP Addresses .	300
Making the Decision	300
Applying the Decision	300
Lesson Summary	301
Lesson 3: Designing RIS Security	302
Designing RIS Security	302
Assessing Security Risks for Remote Installation	303
Making the Decision	307
Applying the Decision	308
Lesson Summary	308
Lesson 4: Designing SNMP Security	309
Designing SNMP Security	309
Assessing the Security Risks of SNMP	310
Restricting Management to Specific SNMP Communities	310
Restricting Management to Specific SNMP Management Stations ...	311
Protecting SNMP Messages from Interception	312
Making the Decision	312
Applying the Decision	312
Lesson Summary	313

Lesson 5: Designing Terminal Services Security	314
Designing Terminal Services Security	314
Assessing Security Risks of Terminal Services	314
Restricting Remote Administration	315
Restricting Access to the Local File System	315
Determining Where to Deploy Terminal Services	315
Implementing Individual User Security	315
Securing Transmissions Between Terminal Services Clients and the Terminal Server	316
Planning for Loss of Strong Authentication Methods	317
Making the Decision	317
Applying the Decision	318
Lesson Summary	318
Lab 9-1: Planning Security for Network Services	319
Lab Objectives	319
About This Lab	319
Before You Begin	319
Scenario: Contoso Ltd.	319
Exercise 1: Designing DNS Security	325
Exercise 2: Designing DHCP Security	326
Exercise 3: Designing RIS Security	326
Exercise 4: Designing SNMP Security	327
Exercise 5: Designing Terminal Services	328
Review	329
 Chapter 10 Planning a Public Key Infrastructure	331
About This Chapter	331
Before You Begin	331
Chapter Scenario: Blue Yonder Airlines	332
Blue Yonder Airlines Destinations	332
The Ordering Web Site	333
Creating Customer Accounts	333
Certificate Management	334
Using the Smart Card	335
Other Uses for PKI at Blue Yonder Airlines	335
Lesson 1: Planning a Certification Authority Hierarchy	336
Reviewing PKI Components	336
Determining Whether to Use a Private or Public CA	337
Choosing a Public CA	337
Choosing a Private CA	338

Making the Decision	339
Applying the Decision	339
Determining the Certification Authority Structure	340
Deploying a Rooted Hierarchy	340
Deploying a Cross-Certification Hierarchy	340
Making the Decision	343
Applying the Decision	343
Planning the Scope of a CA	344
Deploying an Enterprise CA	344
Deploying a Standalone CA	346
Making the Decision	348
Applying the Decision	349
Planning Offline CAs	349
Configuring an Offline Root CA	350
Making the Decision	353
Applying the Decision	353
Designing the Certification Authority Hierarchy	355
Making the Decision	358
Applying the Decision	358
Planning Disaster Recovery of CAs	360
Making the Decision	361
Applying the Decision	361
Lesson Summary	362
Lesson 2: Managing Certification Authorities	363
Planning Certificate Issuance	363
Designing Automatic Issuance	363
Designing Manual Issuance	364
Making the Decision	365
Applying the Decision	365
Planning Certificate Revocation	366
Making the Decision	367
Applying the Decision	368
Planning Certificate Renewal	369
Making the Decision	370
Applying the Decision	371
Lesson Summary	371
Activity: Planning Certificate Renewal Settings	372
Lesson 3: Using Certificates for Authentication	373
Planning Smart Card Logon	373
Planning Smart Card Deployment	374

Defining Permissions for Certificate Templates	374
Configuring CAs to Issue the Required Certificates	375
Acquiring the Required Certificates	376
Defining the Enrollment Process	376
Making the Decision	377
Applying the Decision	377
Planning Certificate-Based Web Authentication	378
Making the Decision	379
Applying the Decision	380
Lesson Summary	380
Lab 10-1: Planning a PKI Deployment	381
Lab Objectives	381
About This Lab	381
Before You Begin	381
Scenario: Contoso Ltd.	381
Exercise 1: Designing a CA Hierarchy for Contoso Ltd.	383
Exercise 2: Planning Security for Web-Based Subscriptions to Magazines	384
Exercise 3: Planning Partner Access	385
Review	386
Chapter 11 Securing Data at the Application Layer	389
About This Chapter	389
Before You Begin	389
Chapter Scenario: Fabrikam Inc.	390
Client Operating Systems	390
The Department of Defense	391
Ongoing Projects	392
Lesson 1: Planning Authenticity and Integrity of Transmitted Data	393
Providing Authenticity and Integrity of Transmitted Data	393
Planning SMB Signing	393
Planning the Deployment of SMB Signing	395
Making the Decision	400
Applying the Decision	400
Planning Digital Signing	402
Determining Protocol Choices for Digital Signing	404
Deploying Public Keys	405
Making the Decision	405
Applying the Decision	405
Lesson Summary	406

Lesson 2: Planning Encryption of Transmitted Data	407
Planning Secure E-Mail Encryption	407
Analyzing the E-Mail Encryption Process	408
Determining Encryption Levels for E-Mail Encryption	408
Determining Protocol Choices for E-Mail Encryption	409
Making the Decision	409
Applying the Decision	410
Planning Application-Level Encryption with SSL/TLS	410
Deploying SSL and TLS	412
Making the Decision	414
Applying the Decision	415
Lesson Summary	416
Activity: Determining Key Usage	417
Lab 11-1: Providing Application-Layer Security for Contoso Ltd.	419
Lab Objectives	419
About This Lab	419
Before You Begin	419
Scenario: Contoso Ltd.	419
Exercise 1: Planning SMB Signing for Contoso Ltd.	421
Exercise 2: Designing Secure E-Mail for Contoso	422
Exercise 3: Planning a Secure Web Site	422
Review	424
 Chapter 12 Securing Data with Internet Protocol Security (IPSec)	427
About This Chapter	427
Before You Begin	427
Chapter Scenario: Fabrikam Inc.	428
The Network	428
Connecting to A. Datum Corporation	428
The Data Collection Package	429
Lesson 1: Designing IPSec Policies	430
Describing IPSec Communications	430
Planning IPSec Protocols	432
Assessing AH	432
Deploying AH	433
Assessing Encapsulating Security Payloads (ESP)	433
Deploying ESP	435
Making the Decision	436
Applying the Decision	437

Planning IPsec Modes	438
Examining Tunnel Mode Packets	440
Making the Decision	441
Applying the Decision	441
Designing IPsec Filters	442
Determining IPsec Exclusions	444
Making the Decision	444
Applying the Decision	445
Designing IPsec Filter Actions	447
Making the Decision	449
Applying the Decision	449
Designing IPsec Encryption and Integrity Algorithms	451
Making the Decision	452
Applying the Decision	452
Designing IPsec Authentication	453
Making the Decision	453
Applying the Decision	454
Lesson Summary	454
Activity: Evaluating IPsec Scenarios	455
Lesson 2: Planning IPsec Deployment	457
Assessing the Preconfigured IPsec Policies	457
Making the Decision	458
Applying the Decision	458
Deploying IPsec Policies in a Workgroup Environment	459
Making the Decision	459
Applying the Decision	460
Deploying IPsec Policies in a Domain Environment	460
Making the Decision	460
Applying the Decision	461
Automatically Deploying Computer Certificates	461
Making the Decision	462
Applying the Decision	463
Troubleshooting IPsec Problems	464
Making the Decision	465
Applying the Decision	466
Lesson Summary	466
Lab 12-1: Designing IPsec Security	467
Lab Objectives	467
About This Lab	467

Before You Begin	467
Scenario: Contoso Ltd.	467
Exercise 1: Designing IPSec Policies for Contoso Ltd.	470
Exercise 2: Planning Deployment of the IPSec Policies	473
Review	475
Chapter 13 Securing Access for Remote Users and Networks	477
About This Chapter	477
Before You Begin	477
Chapter Scenario: Hanson Brothers	478
Providing Access to Home Users	478
Providing Access to the Partner Organization	480
Connecting the Montréal Office	480
Lesson 1: Planning Remote Access Security	481
Choosing Between Dial-Up and VPN Solutions	481
Making the Decision	482
Applying the Decision	483
Planning Remote Access Authentication	483
Making the Decision	484
Applying the Decision	486
Planning Dial-Up Protocols	486
Making the Decision	487
Applying the Decision	487
Planning VPN Protocols	487
Analyzing VPN Protocol Selections	487
Making the Decision	490
Applying the Decision	491
Planning Integration with Windows NT 4.0 Remote Access Service (RAS) Servers	492
Making the Decision	494
Applying the Decision	494
Lesson Summary	494
Lesson 2: Designing Remote Access Security for Users	495
Planning User Settings for Dial-Up Networking Security	495
Making the Decision	496
Applying the Decision	497
Authorizing Dial-Up Connections	498
Making the Decision	499
Applying the Decision	499

Securing Client Configuration	499
Making the Decision	500
Applying the Decision	501
Lesson Summary	501
Lesson 3: Designing Remote Access Security for Networks	502
Choosing Remote Office Connectivity Solutions	502
Making the Decision	503
Applying the Decision	503
Securing Dedicated WAN Connections	503
Making the Decision	504
Applying the Decision	505
Designing VPN Solutions	505
Making the Decision	508
Applying the Decision	509
Lesson Summary	510
Lesson 4: Designing Remote Access Policy	511
Designing Remote Access Policy Condition Attributes	511
Making the Decision	512
Applying the Decision	513
Designing Remote Access Policy Profiles	513
Making the Decision	515
Applying the Decision	515
Planning Remote Access Policy Application	516
Remote Access Policy Application in Mixed Mode	517
Remote Access Policy Application in Native Mode	517
Making the Decision	518
Applying the Decision	518
Lesson Summary	518
Activity: Designing Remote Access Policy	519
Lesson 5: Planning RADIUS Security	521
Introducing RADIUS Authentication	521
Designing RADIUS Deployments	521
Making the Decision	524
Applying the Decision	524
Planning Centralized Application of Remote Access Policy	525
Making the Decision	527
Applying the Decision	528
Lesson Summary	528
Lab 13-1: Designing Security for Remote Access Users	529

Lab Objectives	529
About This Lab	529
Before You Begin	529
Scenario: Contoso Ltd.	529
Exercise 1: Securing Access for the Remote Sales Force	531
Exercise 2: Securing the Connection to the Barcelona Office	535
Review	537
Chapter 14 Securing an Extranet	539
About This Chapter	539
Before You Begin	539
Chapter Scenario: Market Florist	540
Market Florist's DNS Services	540
Market Florist's FTP Server	540
Market Florist's Internet-Accessible Resources	540
External DNS Resource Records	542
The Flower Power Application	542
Lesson 1: Identifying Common Firewall Strategies	543
Identifying Firewall Features to Protect the Extranet	543
Protecting Private Network Addressing with NAT	544
Packet Filters	545
Static Address Mapping	547
Stateful Inspection	547
Advanced Techniques	548
Making the Decision	548
Applying the Decision	549
Comparing DMZ Configurations	551
Designing a Three-Pronged Firewall DMZ	552
Mid-ground DMZ	553
Hybrid DMZ	553
Making the Decision	555
Applying the Decision	555
Lesson Summary	556
Activity: Identifying Firewall Features	557
Lesson 2: Securing Internet-Accessible Resources in a DMZ	559
Securing IIS	559
Making the Decision	562
Applying the Decision	563
Securing Other Services Within the DMZ	565

Making the Decision	567
Applying the Decision	567
Lesson Summary	568
Lesson 3: Securing Data Flow Through a DMZ	569
Determining a Firewall Strategy	569
Making the Decision	570
Applying the Decision	570
Securing DNS Resolution Traffic	570
Making the Decision	572
Applying the Decision	573
Securing Web Traffic	573
Making the Decision	574
Applying the Decision	575
Securing FTP Traffic	575
Making the Decision	576
Applying the Decision	577
Securing Mail Traffic	577
Making the Decision	579
Applying the Decision	580
Securing Application Traffic	581
Making the Decision	584
Applying the Decision	584
Securing Terminal Server Traffic	585
Making the Decision	586
Applying the Decision	586
Securing VPN Traffic	587
Securing PPTP Tunnel Traffic	587
Securing L2TP/IPSec Tunnel Traffic	589
Making the Decision	592
Applying the Decision	592
Lesson Summary	593
Lab 14-1: Designing Firewall Rules	594
Lab Objectives	594
About This Lab	594
Before You Begin	594
Scenario: Contoso Ltd.	594
Exercise 1: Planning the DMZ Configuration	596
Exercise 2: Designing Packet Filters for the DMZ	597
Review	605

Chapter 15 Securing Internet Access	607
About This Chapter	607
Before You Begin	607
Chapter Scenario: Wide World Importers	608
Wide World Importers Domain Model	608
Computers Permitted to Access the Internet	609
Wide World Importers Computers and Applications	610
Wide World Importers Internet Use Policy	610
Wide World Importers Internet Restrictions	610
Security Concerns for Wide World Importers	611
Lesson 1: Designing an Internet Acceptable Use Policy	612
Determining Contents of the Policy	612
Making the Decision	614
Applying the Decision	614
Lesson Summary	614
Lesson 2: Securing Access to the Internet by Private Network Users	615
Identifying Risks When Private Network Users Connect to the Internet	615
Making the Decision	617
Applying the Decision	617
Restricting Internet Access to Specific Computers	618
Making the Decision	619
Applying the Decision	621
Restricting Internet Access to Specific Users	622
Providing Proxy Services	622
Authenticating Proxy Server Requests	623
Making the Decision	624
Applying the Decision	625
Restricting Internet Access to Specific Protocols	627
Restricting Protocol Access in the Web Proxy	627
Restricting Protocol Access in the WinSock Proxy	628
Making the Decision	628
Applying the Decision	629
Lesson Summary	629
Activity: Identifying Security Design Risks	630
Lesson 3: Restricting Access to Content on the Internet	634
Preventing Access to Specific Web Sites	634
Making the Decision	635
Applying the Decision	635

Using the Internet Explorer Administration Kit to Preconfigure Settings	635
Making the Decision	636
Applying the Decision	636
Managing Content Downloads	637
Making the Decision	638
Applying the Decision	638
Preventing Access to Specific Types of Content	639
Making the Decision	640
Applying the Decision	640
Lesson Summary	640
Lesson 4: Auditing Internet Access	641
Designing Proxy Server Auditing	641
Making the Decision	643
Applying the Decision	643
Lesson Summary	643
Lab 15-1: Designing Secure Internet Access	644
Lab Objectives	644
About This Lab	644
Before You Begin	644
Scenario: Contoso Ltd.	644
Exercise 1: Evaluating the Internet Acceptable Use Policy	647
Exercise 2: Designing Firewall Packet Filters for Secure Internet Access	648
Exercise 3: Restricting Access to Content	649
Review	651
Chapter 16 Securing Access in a Heterogeneous Network Environment	653
About This Chapter	653
Before You Begin	654
Chapter Scenario: Blue Yonder Airlines	655
Macintosh Deployment at Blue Yonder Airlines	655
UNIX Deployment at Blue Yonder Airlines	655
A Recent Acquisition	656
Lesson 1: Providing Interoperability Between Windows 2000 and Heterogeneous Networks	657
AppleTalk Network Integration Services	657
Microsoft Services for NetWare 5.0	657
Microsoft Services for UNIX 2.0	658
Making the Decision	659

Applying the Decision	659
Lesson Summary	660
Lesson 2: Securing Authentication in a Heterogeneous Network	661
Securing Authentication for Macintosh Clients	661
Making the Decision	662
Applying the Decision	662
Securing Authentication for Novell Clients	663
Making the Decision	664
Applying the Decision	664
Securing Authentication for UNIX Clients	664
Making the Decision	665
Applying the Decision	666
Lesson Summary	667
Activity: Identifying Authentication Risks in a Heterogeneous Network Environment	668
Lesson 3: Designing Directory Synchronization and Integration	669
Synchronizing Active Directory with a Novell Directory	669
Making the Decision	669
Applying the Decision	670
Securely Synchronizing Multiple Directories	670
Making the Decision	671
Applying the Decision	671
Integrating Active Directory with Kerberos Realms	672
Making the Decision	674
Applying the Decision	675
Lesson Summary	675
Lesson 4: Securing Access to Windows 2000 Resources	676
Securing Macintosh Access to Windows 2000 Resources	676
Securing File Access	676
Securing Print Access	677
Making the Decision	677
Applying the Decision	678
Securing NetWare Access to Windows 2000 Resources	678
Securing File Access	678
Securing Print Access	679
Making the Decision	679
Applying the Decision	679
Securing UNIX Access to Windows 2000 Resources	680
Securing File Access	680

Securing Print Access	681
Making the Decision	681
Applying the Decision	682
Lesson Summary	682
Lesson 5: Securing Windows 2000 User Access to Heterogeneous Networks	683
Securing Access to NetWare Resources	683
Providing Access to NetWare Resources by Using a Native Client ...	684
Providing Access to NetWare Resources by Using a Gateway	686
Making the Decision	687
Applying the Decision	688
Securing Access to UNIX Resources	689
Providing Access to UNIX Resources with UNIX Client Software ...	689
Providing Access to UNIX Resources by Using a Gateway	689
Making the Decision	690
Applying the Decision	690
Lesson Summary	691
Lab 16-1: Securing Heterogeneous Clients	692
Lab Objectives	692
About This Lab	692
Before You Begin	692
Scenario: Contoso Ltd.	692
Exercise 1: Securing Macintosh User Access	695
Exercise 2: Securing Access to NetWare Resources	696
Exercise 3: Securing UNIX User Access	698
Review	699
Chapter 17 Designing a Security Plan	701
About This Chapter	701
Before You Begin	701
Chapter Scenario: Fabrikam Inc.	702
The Internal Audit	702
The Radar System Project	703
The Team	704
Lesson 1: Defining a Security Policy	705
Making the Decision	707
Applying the Decision	707
Lesson Summary	708
Lesson 2: Developing a Security Plan	709
Making the Decision	710

Applying the Decision	711
Lesson Summary	712
Lesson 3: Maintaining a Security Plan	713
Making the Decision	714
Applying the Decision	715
Lesson Summary	715
Review	716
Appendix: Answers	717
Index	771