Contents

Understand how ISA Server fits into .NET

Just as Proxy Server was considered a member of the Microsoft BackOffice Family, ISA Server also belongs to a new Microsoft "family," the members of which are designed to work with Windows 2000 in an enterprise environment. This group of enterprise servers is now called the Microsoft.Net family, or simply ".Net" (pronounced dot-net) servers.

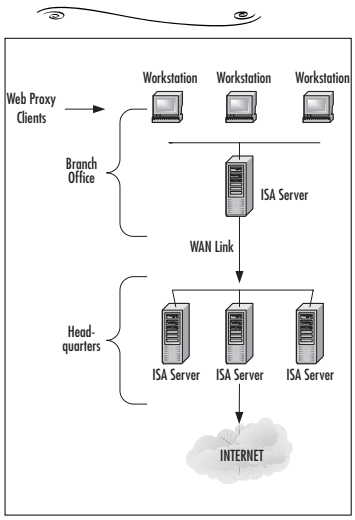
Introduction

Chapter 1 Introduction to Microsoft ISA Server **1**

What Is ISA Server? 2
Why "Security and Acceleration" Server? 3
Internet Security 3
Internet Acceleration 8
The History of ISA: Microsoft Proxy Server 9
In the Beginning: Proxy Server, Version 1.0 9
Getting Better All the Time: Proxy Server, Version 2.0 10
A New Name for New and Improved Functionality: Proxy Server 3.0 (ISA Server) 11
ISA Server Options 15
ISA Standard Edition 15
ISA Enterprise Edition 16
ISA Server Installation Modes 18

The Microsoft.Net Family of Enterprise Servers 19
The Role of ISA Server in the Network Environment 22
An Overview of ISA Server Architecture 22
Layered Filtering 24
ISA Client Types 29
ISA Server Authentication 38
ISA Server Features Overview 43
Firewall Security Features 43
Firewall Features Overview 44
System Hardening 45
Secure, Integrated VPN 46
Integrated Intrusion Detection 49
Web Caching Features 51
Internet Connection-Sharing Features 52
Unified Management Features 52
Extensible Platform Features 55
Who This Book Is For and What It Covers 56
Summary 60
Solutions Fast Track 61
Frequently Asked Questions 65

Find complete coverage of ISA Server in the Enterprise including hierarchical caching



Chapter 2 ISA Server in the Enterprise 69
Introduction 70
Enterprise-Friendly Features 70
Reliability 71
Scalability 72
Scaling Up 73
Scaling Out 73
Scaling Down 73
Multiprocessor Support 73
The Advantages of Multiprocessing 73
Why Symmetric Multiprocessing? 75
Network Load-Balancing Support 76
Clustering 77
Hierarchical and Distributed Caching 77
Total Cost of Ownership 81
Designing Enterprise Solutions 83
General Enterprise Design Principles 84

Enterprise Core Services and Protocols 84
The Enterprise Networking Model 85
Enterprise Technologies 89
ISA Server Design Considerations 91
Planning Multiserver Arrays 104
Understanding Multiserver Management 104
Backing Up the Array Configuration Information 105
Using Tiered Policy 108
Planning Policy Elements 108
Understanding ISA Server Licensing 110
Summary 113
Solutions Fast Track 114
Frequently Asked Questions 118

Chapter 3 Security Concepts and Security Policies 121
Introduction 122
Security Overview 122
Defining Basic Security Concepts 123
Knowledge Is Power 123
Think Like a Thief 124
The Intrusion Triangle 125
Removing Intrusion Opportunities 126
Security Terminology 127
Addressing Security Objectives 129
Controlling Physical Access 130
Physical Access Factors 130
Physical Security Summary 139
Preventing Accidental Compromise of Data 140
Know Your Users 140
Educate Your Users 140
Control Your Users 141
Preventing Intentional Internal Security Breaches 141
Hiring and Human Resource Policies 142
Detecting Internal Breaches 142

Preventing Intentional Internal Breaches 145
Preventing Unauthorized External Intrusions and Attacks 145
External Intruders with Internal Access 146
Tactical Planning 146
Recognizing Network Security Threats 147
Understanding Intruder Motivations 147
Recreational Hackers 147
Profit-Motivated Hackers 148
Vengeful Hackers 149
Hybrid Hackers 149
Classifying Specific Types of Attacks 150
Social Engineering Attacks 150
Denial-of-Service Attacks 152
Scanning and Spoofing 161
Source-Routing Attack 164
Other Protocol Exploits 165
System and Software Exploits 165
Trojans, Viruses, and Worms 166
Categorizing Security Solutions 168
Hardware Security Solutions 168
Hardware-Based Firewalls 168
Other Hardware Security Devices 168
Software Security Solutions 169
Windows 2000 Security Features 169
Security Software 169
Designing a Comprehensive Security Plan 170
Evaluating Security Needs 171
Assessing the Type of Business 172
Assessing the Type of Data 172
Assessing the Network Connections 173
Assessing Management Philosophy 173
Understanding Security Ratings 174
Legal Considerations 175
Designating Responsibility for Network Security 176
Responsibility for Developing the Security Plan and Policies 176

See how to incorporate ISA Server in your security plan

ISA Server's firewall function prevents unauthorized packets from entering your internal network. ISA also provides monitoring of intrusion attempts as well as allowing you to set alerts to notify you when intrusions occur. This chapter also covers system hardening, Secure Sockets Layer, SSL tunneling, and SSL bridging.

Responsibility for Implementing and Enforcing the Security Plan and Policies 176
Designing the Corporate Security Policy 177
Developing an Effective Password Policy 178
Educating Network Users on Security Issues 182
Incorporating ISA Server into Your Security Plan 182
ISA Server Intrusion Detection 182
Implementing a System-Hardening Plan with ISA 184
System-Hardening Goals and Guidelines 185
Using the Security Configuration Wizard 186
Using SSL Tunneling and Bridging 187
SSL Tunneling 187
SSL Bridging 188
Summary 192
Solutions Fast Track 193
Frequently Asked Questions 198

Chapter 4 ISA Server Deployment Planning and Design 201
Introduction 202
ISA Deployment: Planning and Designing Issues 202
Assessing Network and Hardware Requirements 202
System Requirements 203
Software Requirements 203
Processor Requirements 204
Multiprocessor Support 205
RAM Configuration 206
Disk Space Considerations 208
Cache Size Considerations 208
Logging and Reporting 209
Network Interface Configuration 210

Active Directory Implementation 216
Mission-Critical Considerations 217
Hard Disk Fault Tolerance 217
Mirrored Volumes (Mirror Sets) 218
RAID 5 Volumes (Stripe Sets with Parity) 219
Network Fault Tolerance 223
Server Fault Tolerance 224
Bastion Host Configuration 227
Planning the Appropriate Installation Mode 228
Installing in Firewall Mode 229
Installing in Cache Mode 229
Installing in Integrated Mode 230
Planning for a Standalone or an Array Configuration 231
Planning ISA Client Configuration 233
The Firewall Client 233
The Web Proxy Client 235
The SecureNat Client 236
Assessing the Best Solution for Your Network 236
Internet Connectivity and DNS Considerations 238
Level of Service 238
External Interface Configuration 239
DNS Issues 240
Summary 242
Solutions Fast Track 242
Frequently Asked Questions 246

Chapter 5 ISA Server Installation 249
Introduction 250
Installing ISA Server on a Windows 2000 Server 250
Putting Together Your Flight Plan 250
Installation Files and Permissions 251
CD Key and Product License 251
Active Directory Considerations 252
Server Mode 253
Disk Location for ISA Server Files 253

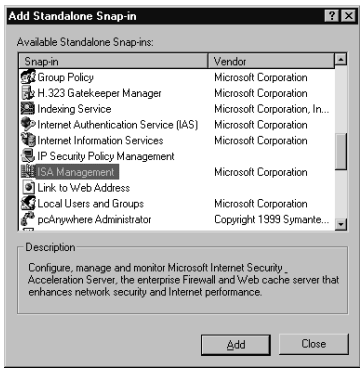
Understand the differences between Proxy Server 2.0 and ISA Server

- IPX/SPX is not supported.
- The Web Proxy Service listens on Port 8080 and Web proxy client implications.
- The Winsock client is not required on published servers.
- The Web cache is stored as a single file.
- There is no SOCKS service.
- The firewall client doesn't support 16-bit operating systems.
- There are incompatibilities between ISA and IIS on same machine.

Internal Network IDs and the Local Address Table 254
ISA Server Features Installation 254
Performing the Installation 255
Installing ISA Server: A Walkthrough 255
Upgrading a Standalone Server to an Array Member: A Walkthrough 267
Performing the Enterprise Initialization 268
Backing Up a Configuration and Promoting a Standalone Server to an Array Member 271
Changes Made After ISA Server Installation 278
Migrating from Microsoft Proxy Server 2.0 278
What Gets Migrated and What Doesn't 278
Functional Differences Between Proxy Server 2.0 and ISA Server 281
Learn the ISA Server Vocabulary 285
Upgrading Proxy 2.0 on the Windows 2000 Platform 286
Upgrading a Proxy 2.0 Installation on Windows NT 4.0 290
A Planned Upgrade from Windows NT 4.0 Server to Windows 2000 290
Summary 293
Solutions Fast Track 294
Frequently Asked Questions 297

Chapter 6 Managing ISA Server 299
Introduction 300
Understanding Integrated Administration 300
The ISA Management Console 301
Adding ISA Management to a Custom MMC 302
The Components of the ISA MMC 305
The ISA Console Objects 312
ISA Wizards 330
The Getting Started Wizard 330

Everything you need to manage ISA Server



ISA Management can be added to a custom MMC.

Rules Wizards 330
VPN Wizards 331
Performing Common Management Tasks 332
Configuring Object Permissions 332
Default Permissions 332
Special Object Permissions 332
Setting Permissions on ISA Objects 334
Managing Array Membership 335
Creating a New Array 335
Adding and Removing Computers 335
Promoting a Standalone ISA Server 336
Using Monitoring, Alerting, Logging, and Reporting Functions 337
Creating, Configuring, and Monitoring Alerts 338
Viewing Alerts 338
Creating and Configuring Alerts 338
Refreshing the Display 343
Event Messages 343
Monitoring Sessions 344
Using Logging 345
Logging to a File 345
Logging to a Database 346
Configuring Logging 348
Generating Reports 351
Creating Report Jobs 351
Viewing Generated Reports 356
Configuring Sort Order for Report Data 362
Saving Reports 362
Configuring the Location for Saving the Summary Database 363
Understanding Remote Administration 365
Installing the ISA Management Console 365
Managing a Remote Standalone Computer 365
Remotely Managing an Array or Enterprise 366
Using Terminal Services for Remote Management of ISA 367

Installing Terminal Services on the ISA Server 367
Installing Terminal Services Client Software 369
Summary 372
Solutions Fast Track 373
Frequently Asked Questions 375

Chapter 7 ISA Architecture and Client Configuration 377

Introduction 378
Understanding ISA Server Architecture 379
The Web Proxy Service 380
The Firewall Service 382
How the Firewall Service Works 382
The Network Address Translation Protocol Driver 384
The Scheduled Content Download Service 385
ISA Server Services Interactions 386
Configuration Changes and ISA Server Services Restarts 388
Installing and Configuring ISA Server Clients 390
The SecureNAT Client 390
SecureNAT Clients on Simple Networks 391
SecureNAT Clients on "Not-Simple" Networks 392
Limitations of the SecureNAT Client 394
Manually Configuring the SecureNAT Client 396
Configuring the SecureNAT Client via DHCP 397
The Firewall Client 398
Advantages of Using the Firewall Client 398
Disadvantages of Using the Firewall Client 399

Hundreds of security alerts, undocumented hints, and ISA Server mysteries make sure you don't miss a thing

SECURITY ALERT!

SecureNAT clients must be configured with the address of a DNS server that can resolve Internet names. You can use a DNS server located on the Internet (such as your ISP's DNS server), or you can configure an internal DNS server to use a forwarder on the Internet. Unlike the RRAS NAT Service, the ISA server does not perform DNS Proxy Services for the SecureNAT clients.

DNS Configuration Issues for Firewall Clients 401
Deploying the Firewall Client 403
Manual Installation of a Firewall Client via URL 404
Command-Line Parameters for a Scripted Installation 407
Automatic Installation 408
Configuring the Firewall Client 411
Automating the Configuration of the Firewall Client 413
Firewall Service Client Configuration Files 423
The Web Proxy Client 428
Why You Should Configure the Web Proxy Client 428
DNS Considerations for the Web Proxy Client 430
Configuring the Web Proxy Client 430
Autodiscovery and Client Configuration 433
Summary 435
Solutions Fast Track 437
Frequently Asked Questions 440

Chapter 8 Configuring ISA Server for Outbound Access 443
Introduction 444
Configuring the Server for Outbound Access 444
Configuring Listeners for Outbound Web Requests 445
Server Performance 448
Network Configuration Settings 449
Firewall Chaining: Routing SecureNAT and Firewall Client Requests 449
Configuring Firewall and SecureNAT Client Routing 450
Routing Web Proxy Client Requests 453
Configuring a Web Proxy Service Routing Rule 454
Routing to a Linux Squid Server 461

Answers all your questions about configuring outbound access

Q: I want to prevent users from gaining access to .MP3 files from the Napster site. Is there an easy way to do this?

A: Yes. Configure a site and content rule that prevents downloading of .MP3 files. If you are interested in blocking only .MP3 files, you can create a new content group in the Policy Elements node and then use this content group to create the site and content rule to limit the download of .MP3s.

Configuring ISA Web Proxy Chaining 463
Configuring Routing for ISA Server Chains 466
Outbound PPTP Requests 468
The Local Address Table 470
Configuring the LAT 471
Building the Routing Table 473
Configuring the Local Domain Table 475
Creating Secure Outbound Access Policy 477
Creating and Configuring Policy Elements 479
Dial-up Entries 480
Bandwidth Priorities 484
Schedules 487
Destination Sets 489
Client Address Sets 492
Protocol Definitions 494
Content Groups 498
Creating Rules Based on Policy Elements 501
Bandwidth Rules 502
Creating a Bandwidth Rule 503
Managing Bandwidth Rules 507
Site and Content Rules 509
Creating a Site and Content Rule 509
Managing Site and Content Rules 513
Protocol Rules 516
Protocol Rules Depend on Protocol Definitions 516
Creating a Protocol Rule 517
Creating a Protocol Rule to Allow Multiple Protocol Definitions: PCAnywhere 9.x 520
Creating a Protocol Rule to Allow Access to Multiple Primary Port Connections 522
Managing Protocol Rules 522
IP Packet Filters 523
Dynamic Packet Filtering 524
Packet Filters for Network Services Located on the ISA Server 524

Configuring Application Filters That Affect Outbound Access 528
FTP Access Filter 528
HTTP Redirector Filter 530
SOCKS Filter 534
Streaming Media Filter 535
Live Stream Splitting 536
Understanding and Configuring the Web Proxy Cache 538
Cache Configuration Elements 539
Configuring HTTP Caching 539
Configuring FTP Caching 541
Configuring Active Caching 542
Configuring Advanced Caching Options 544
Scheduled Content Downloads 546
Summary 551
Solutions Fast Track 552
Frequently Asked Questions 555

Chapter 9 Configuring ISA Server for Inbound Access 557
Introduction 558
Configuring ISA Server Packet Filtering 558
How Packet Filtering Works 558
Default Packet Filters 559
When Packet Filtering Is Disabled 559
Static versus Dynamic Packet Filtering 559
When to Manually Create Packet Filters 560
Enabling Packet Filtering 561
Creating Packet Filters 561
Managing Packet Filters 569
Supporting Applications on the ISA Server 571
Publishing Services on Perimeter Networks Using Packet Filters 573
Packet Filtering Options 575
Routing between Public and Private Networks 575
Packet Filtering/Routing Scenarios 576
Packet Filtering Enabled with IP Routing Enabled 578

The Packet Filters Tab 578
Enabling Intrusion Detection 580
Application Filters That Affect Inbound Access 581
DNS Intrusion Detection Filter 581
Configuring the H.323 Filter 582
POP Intrusion Detection Filter 583
RPC Filter 583
SMTP Filter 584
The General Tab 584
The Attachments Tab 584
The Users/Domains Tab 587
Configuring the SMTP Message Screener 587
Designing Perimeter Networks 595
Limitations of Perimeter Networks 595
Perimeter Network Configurations 596
Back-to-Back ISA Server Perimeter Networks 596
Tri-homed ISA Server Perimeter Networks 599
Publishing Services on a Perimeter Network 600
Publishing FTP Servers on a Perimeter Network 602
Enabling Communication between Perimeter Hosts and the Internal Network 603
Bastion Host Considerations 604
Configuring the Windows 2000 Bastion Host 604
Summary 607
Solutions Fast Track 607
Frequently Asked Questions 609

Chapter 10 Publishing Services to the Internet 611

Introduction 612
Types of Publishing 612
Web Publishing 612
Server Publishing 613
Publishing Services on a Perimeter Network 614
Web Server Publishing 615
Preparing to Publish 615

DNS Entries 615
DNS Client/Server Infrastructure 616
Destination Sets 618
ISA Client Configuration 620
Configuring the Inbound Web Requests Listener 621
Web Publishing Walkthrough—Basic Web Publishing 627
Publishing a Web Site on the ISA Server 630
Readying IIS for Publishing 631
Creating the Publishing Rule 632
Web Publishing through Protocol Redirection 637
Creative Publishing Using Destination Sets 639
Secure Web Site Publishing 642
Terminating the Secure Connection at the ISA Server 643
Bridging Secure Connections as SSL Requests 650
Publishing a Secure Web Site via Server Publishing Rules 653
Publishing Services 653
Limitations of Server Publishing Rules 654
You Can Publish a Service Only Once 654
You Cannot Redirect Ports 655
You Cannot Bind a Particular External Address to an Internal IP Address 655
Server Publishing Bypasses the Web Proxy Service 655
SecureNAT Does Not Work for All Published Servers 656
You Cannot Use Destination Sets in Server Publishing Rules 656
Preparing for Server Publishing 656
Protocol Definitions 657
ISA Client Configuration 657
Client Address Sets 657
Server Publishing Walkthrough—Basic Server Publishing 658
Secure Mail Server Publishing 662

Complete instructions for publishing content on a private network, including undocumented tips

You must configure a packet filter for the TZO client software to work correctly. Remember that all applications on the ISA server that require external network access require static packet filters. The packet filter settings are:

Filter type: Custom
IP protocol: TCP
Direction: Outbound
Local port: Dynamic
Remote port: Fixed Port
Remote port number: 21331

Configuring ISA Server to Support Outlook Web Access 666
Publishing a Terminal Server 667
Terminal Server on the ISA Server 668
Terminal Server on the Internal Network and on the ISA Server 669
Terminal Services Security Considerations 671
Publishing a Web Server Using Server Publishing 672
The H.323 Gatekeeper Service 674
Gatekeeper-to-Gatekeeper Calling 677
ILS Servers 679
NetMeeting Clients on the Internet 680
Configuring the Gatekeeper 682
Creating Destinations 682
Call Routing Rules 684
Managing the Gatekeeper 691
Virtual Private Networking 693
Configuring VPN Client Access 693
Gateway-to-Gateway VPN Configuration 695
Configuring the Local VPN 695
Configuring the Remote VPN 700
Testing the Configuration 702
Summary 704
Solutions Fast Track 706
Frequently Asked Questions 709

Chapter 11 Optimizing, Customizing, Integrating, and Backing Up ISA Server 713
Introduction 714
Optimizing ISA Server Performance 714
Establishing a Baseline and Monitoring Performance 716
How Baselines Are Used 716
Defining Threshold Values 717
Using the Performance Monitor Tools 717
Addressing Common Performance Issues 742
Addressing Network Bandwidth Issues 742
Addressing Load-Balancing Issues 746

Master the Windows Messenger Service

A Network Message Is Sent to the Specified Account When the Alert Is Triggered

Cache Configuration Issues 748
Editing the Windows 2000 Registry to Tune ISA Performance Settings 752
Customizing ISA Server 754
Using the ISA Server Software Developer's Kit 755
Administration Scripts 755
Sample Filters 757
Using Third-Party Add-ons 758
Types of Add-on Programs 758
Overview of Available Add-on Programs 760
Integrating ISA Server with Other Services 760
Understanding Interoperability with Active Directory 761
Standalone versus Array Member 761
The Active Directory Schema 761
ISA Server and Domain Controllers 762
Understanding Interoperability with Routing and Remote Access Services 762
RRAS Components 762
RRAS and ISA Server 763
Understanding Interoperability with Internet Information Server 764
IIS Functionality 764
Publishing IIS to the Internet 764
Understanding Interoperability with IPSecurity 765
How IPSec Works 766
How IPSec Is Configured in Windows 2000 766
IPSec and ISA Server 768
Integrating an ISA Server into a Windows NT 4.0 Domain 769
Backing Up and Restoring the ISA Configuration 769
Backup Principles 769
Backing Up and Restoring Standalone Server Configurations 770
Backing Up and Restoring Array and Enterprise Configurations 771
Backing Up and Restoring an Array Configuration 772

Backing Up and Restoring an Enterprise Configuration 773
Summary 775
Solutions Fast Track 776
Frequently Asked Questions 780

Chapter 12 Troubleshooting ISA Server 783
Introduction 784
Understanding Basic Troubleshooting Principles 785
Troubleshooting Guidelines 786
The Five Steps of Troubleshooting 786
Troubleshooting Tips 791
ISA Server and Windows 2000 Diagnostic Tools 793
ISA Server Troubleshooting Resources 795
Troubleshooting ISA Server Installation and Configuration Problems 802
Hardware and Software Compatibility Problems 802
ISA Server Doesn't Meet Minimum System Requirements 803
ISA Server Exhibits Odd Behavior When Windows 2000 NAT Is Installed 803
Internal Clients Are Unable to Access External Exchange Server 804
Initial Configuration Problems 804
Unable to Renew DHCP Lease 804
Failure of Services to Start After Completing Installation 805
Inability to Join Array 805
Inability to Save LAT Entry 806
ISA Server Control Service Does Not Start 806
Troubleshooting Authentication and Access Problems 807
Authentication Problems 807
User's HTTP Request Is Sometimes Allowed, although a Site and Content Rule Denies Access 808

Find step-by-step instructions for troubleshooting ISA Server

1. Information gathering
2. Analysis and planning
3. Implementation of a solution
4. Assessment of the effectiveness of the solution
5. Documentation of the incident

Failure to Authenticate Users of Non-Microsoft Browsers 809
Error Message When Using Pass-Through Authentication with NTLM 810
Access Problems 810
Inability of Clients to Browse External Web Sites 811
Problems with Specific Protocols or Protocol Definitions 811
Inability of Clients to PING External Hosts 812
Redirection of URL Results in Loop Condition 812
Ability of Clients to Continue Using a Specific Protocol After Disabling of Rule 813
Dial-up and VPN Problems 813
Inability of ISA Server to Dial Out to the Internet 813
Dial-up Connection Is Dropped 814
Inability of PPTP Clients to Connect through ISA Server 814
Troubleshooting ISA Client Problems 815
Client Performance Problems 815
Slow Client Connection: SecureNAT Clients 815
Slow Internal Connections: Firewall Clients 816
Client Connection Problems 816
Inability of Clients to Connect via Modem 817
Inability of SecureNAT Clients to Connect to the Internet 817
Inability of Clients to Connect to External SSL Sites 818
Inability of SecureNAT Clients to Connect Using Computer Names 819
Inability of SecureNAT Clients to Connect to a Specific Port Due to a Timeout 819

Troubleshooting Caching and Publishing Problems 820
Caching Problems 820
All Web Objects Not Being Cached 820
Web Proxy Service Does Not Start 821
Publishing Problems 821
Inability of Clients to Access Published Web Server 822
Inability of External Clients to Send E-mail via Exchange Server 822
Summary 824
Solutions Fast Track 824
Frequently Asked Questions 828

Appendix ISA Server 2000 Fast Track 831

Index 869