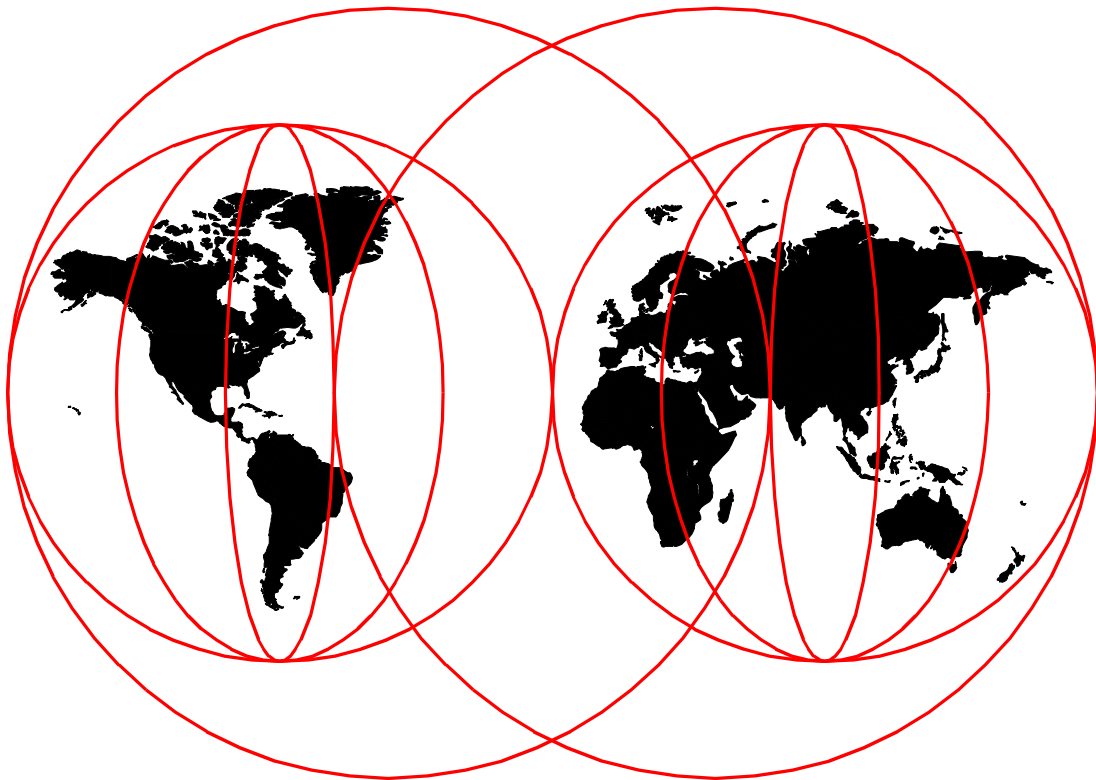


AS/400 Mail: Multiple SMTP Domains Behind a Firewall

Fant Steele, Marc Jenni



International Technical Support Organization

<http://www.redbooks.ibm.com>



International Technical Support Organization

SG24-5643-00

**AS/400 Mail: Multiple SMTP Domains
Behind a Firewall**

December 1999

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix E, "Special notices" on page 353.

First Edition (December 1999)

This edition applies to V4R4 of IBM Firewall for AS/400 5769-FW1, V3.3 of IBM eNetwork Firewall for Windows NT, Lotus Domino R4.6.6, and Lotus Domino R5.0.6 for use with V4R4 of OS/400.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JLU Building 107-2
3605 Highway 52N
Rochester, Minnesota 55901-7829

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1999. All rights reserved.

Note to U.S Government Users - Documentation related to restricted rights - Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	xi
Tables	xix
Preface	xxi
The team that wrote this redbook	xxi
Comments welcome	xxii
Chapter 1. What is new in the IBM Firewall for AS/400 V4R4	1
1.1 Hardware and software requirements	1
1.2 IBM Firewall for AS/400 positioning	1
1.3 IBM Firewall for AS/400 components	2
1.4 IBM Firewall for AS/400 V4R4 enhancements	3
1.4.1 Multiple domain support	3
1.4.2 Multiple mail servers	4
1.4.3 Changes to packet filter log messages	4
1.4.4 Improved operation of the Start button	5
1.4.5 DNS name explanation for V4R4	5
1.4.6 Improved usability due to changes in the NAT MAP setting syntax ..	5
1.4.7 Basic FastPath	6
1.4.8 New IPCS hardware	6
1.4.9 New name for the IPCS and FSIOIP cards	6
1.5 Upgrading IBM Firewall for AS/400 to V4R4	6
1.6 What has changed since IBM Firewall for AS/400 V4R1	7
Chapter 2. Planning your mail environment	9
2.1 Evaluating your current e-mail environment	9
2.2 Making your plan	10
2.3 Scenarios documented in this book	11
2.3.1 One domain with subdomains on a single system	11
2.3.2 Multiple domains on a single system	12
2.3.3 Multiple domains on multiple systems	13
2.3.4 Single domain with fanout to multiple systems	14
Chapter 3. One domain with subdomains on a single system	17
3.1 Scenario	17
3.1.1 Scenario network configuration	17
3.1.2 Scenario objectives	18
3.1.3 Scenario advantages	18
3.1.4 Scenario limitations	18
3.1.5 Planning considerations	19
3.1.6 Task summary	21
3.2 Configuring the AS/400 DNS	21
3.2.1 Task summary	22
3.2.2 Configuring the AS/400 DNS to handle the internal domain	22
3.2.3 Adding systems to the domain	23
3.2.4 Adding the subdomains to the DNS	24
3.2.5 Configuring the MX record for each subdomain	25
3.2.6 Configuring the internal DNS to forward the queries to the firewall ..	26
3.3 Configuring IBM Firewall for AS/400 (FW1MAIL)	27
3.3.1 Scenario network configuration	27

3.3.2	Task summary	28
3.3.3	Installing IBM Firewall for AS/400 (FW1MAIL)	28
3.3.4	Performing basic configuration (FW1MAIL)	29
3.3.5	Planning NAT to map the POP3 server address outside the firewall	33
3.3.6	Configuring NAT	34
3.3.7	Starting NAT and turning on IP forwarding	36
3.3.8	Adding filter rules	37
3.3.9	Restarting filters	38
3.3.10	Filter rules to allow Domino access from the Internet	38
3.4	Configuring IBM eNetwork Firewall for Windows NT (FW1NT)	39
3.4.1	Scenario network configuration	39
3.4.2	Task summary	39
3.4.3	Installing IBM eNetwork Firewall for Windows NT (FW1NT)	40
3.4.4	Setting up IBM eNetwork Firewall for Windows NT	40
3.4.5	Planning NAT to map POP3 server address outside the firewall	51
3.4.6	Configuring the Windows NT system (FW1NT)	52
3.4.7	Configuring NAT	53
3.4.8	Adding new rules	55
3.4.9	Creating a service	56
3.4.10	Creating a network object	58
3.4.11	Creating a connection	58
3.4.12	Activating rules	60
3.4.13	Filter rules to allow Domino access from the Internet	61
3.5	Configuring the SMTP server on the AS/400 system	61
3.5.1	Task summary	61
3.5.2	Setting up SMTP attributes	62
3.5.3	Verifying the HOME400 TCP/IP domain name information	62
3.5.4	Handling multiple SMTP domains on a single AS/400 system	63
3.5.5	Adding the firewall name to the host table entries	64
3.5.6	Starting the SMTP server	64
3.6	Configuring the POP3 server on the AS/400 system	65
3.6.1	Task summary	65
3.6.2	Setting up the POP3 server attributes	65
3.6.3	Configuring a default route to route POP3 server responses	65
3.6.4	Adding POP3 accounts	66
3.6.5	Configuring POP3 accounts	67
3.6.6	POP3 mailboxes	70
3.6.7	Starting the POP3 server	71
3.7	Configuring the Domino server for mail	71
3.7.1	Task summary	71
3.7.2	Planning the Domino server on an AS/400 system	71
3.7.3	Setting up HOME400 to handle Domino	72
3.7.4	Installing Domino server on HOME400	72
3.7.5	Installing Domino Administrator on your workstation	74
3.7.6	Setting up your workstation to administer Domino	78
3.7.7	Configuring Domino server for SMTP mail	82
3.7.8	Linking Domino server with the firewall	85
3.7.9	Creating Lotus Notes mail users	86
Chapter 4.	Multiple domains on a single system	91
4.1	Scenario	91
4.1.1	Scenario network configuration	91
4.1.2	Scenario objectives	92

4.1.3	Scenario advantages	92
4.1.4	Scenario limitations	92
4.1.5	Planning considerations	93
4.1.6	Task summary	95
4.2	Configuring the AS/400 DNS	96
4.2.1	Task summary	96
4.2.2	Configuring the AS/400 DNS to handle the internal domain	96
4.2.3	Adding systems to the domain	97
4.2.4	Adding the mail domains to the DNS	98
4.2.5	Configuring the MX record for each of the three domains	99
4.2.6	Configuring the internal DNS to forward the queries to the firewall	100
4.3	Configuring IBM Firewall for AS/400 (FW2MAIL)	101
4.3.1	Scenario network configuration	101
4.3.2	Task summary	102
4.3.3	Installing IBM Firewall for AS/400 (FW2MAIL)	102
4.3.4	Performing basic configuration (FW2MAIL)	103
4.3.5	Removing MX record for the domain domain.com	107
4.4	Configuring IBM eNetwork Firewall for Windows NT (FW2NT)	109
4.4.1	Scenario network configuration	109
4.4.2	Task summary	109
4.4.3	Installing IBM eNetwork Firewall for Windows NT (FW2NT)	109
4.4.4	Setting up IBM eNetwork Firewall for Windows NT	110
4.5	Configuring the SMTP server on the AS/400 system	122
4.5.1	Task summary	122
4.5.2	Setting up SMTP attributes	122
4.5.3	Verifying the HOME400 TCP/IP domain name information	122
4.5.4	Handling multiple SMTP domains on a single AS/400 system	123
4.5.5	Adding the firewall name to the host table entries	124
4.5.6	Starting the SMTP server	124
4.6	Configuring the POP3 server on the AS/400 system	125
4.6.1	Task summary	125
4.6.2	Setting up the POP3 server attributes	125
4.6.3	Adding POP3 accounts	126
4.6.4	Configuring POP3 accounts	126
4.6.5	POP3 mailboxes	130
4.6.6	Starting the POP3 server	130
4.7	Configuring the Domino server for mail	130
4.7.1	Task summary	130
4.7.2	Configuring Domino server for SMTP mail	131
4.7.3	Linking Domino server with the firewall	134
4.7.4	Creating Lotus Notes mail users	135
Chapter 5. Multiple domains on multiple systems		139
5.1	Scenario	139
5.1.1	Scenario network configuration	139
5.1.2	Scenario objectives	140
5.1.3	Scenario advantages	140
5.1.4	Scenario limitations	141
5.1.5	Planning considerations	141
5.1.6	Task summary	143
5.2	Configuring the AS/400 DNS	144
5.2.1	Task summary	144
5.2.2	Configuring the AS/400 DNS to handle internal domains	144

5.2.3	Adding host names to the domains	146
5.2.4	Configuring the MX record for each domain	147
5.2.5	Configuring the internal DNS to forward the queries to the firewall.	147
5.3	Configuring IBM Firewall for AS/400 (FW3MAIL)	149
5.3.1	Scenario network configuration	149
5.3.2	Task summary	149
5.3.3	Installing IBM Firewall for AS/400 (FW3MAIL)	150
5.3.4	Performing basic configuration (FW3MAIL)	151
5.4	Configuring IBM eNetwork Firewall for Windows NT (FW3NT)	154
5.4.1	Scenario network configuration	154
5.4.2	Task summary	155
5.4.3	Installing IBM eNetwork Firewall for Windows NT (FW3NT)	155
5.4.4	Setting up IBM eNetwork Firewall for Windows NT	155
5.5	Configuring the SMTP server on the AS/400 MAILSRV3	167
5.5.1	Task summary	167
5.5.2	Setting up SMTP attributes	167
5.5.3	Verifying the HOME400 TCP/IP domain name information.	167
5.5.4	Handling the SMTP mail domain on the AS/400 MAILSRV3.	168
5.5.5	Adding the firewall name to the host table entries	169
5.5.6	Starting the SMTP server.	169
5.6	Configuring the POP3 server on the AS/400 MAILSRV3	169
5.6.1	Task summary	170
5.6.2	Setting up the POP3 server attributes	170
5.6.3	Adding POP3 accounts	170
5.6.4	Configuring POP3 accounts	171
5.6.5	POP3 mailboxes	174
5.6.6	Starting the POP3 server.	175
5.7	Planning the Domino server on AS/400 systems	175
5.7.1	Planning considerations.	175
5.8	Configuring the Domino server for mail	176
5.8.1	Task summary	177
5.8.2	Configuring Domino server for SMTP mail	177
5.8.3	Linking the Domino server with the firewall	180
5.8.4	Creating Lotus Notes mail users	181
5.9	Configuring Domino with MSF on the AS/400 system	183
5.9.1	Task summary	183
5.9.2	Setting up SMTP attributes on MAILSRV2	184
5.9.3	Verifying the MAILSRV2 TCP/IP domain name information	184
5.9.4	Handling the SMTP domain using MSF on the AS/400 system.	185
5.9.5	Adding the firewall name to the host table entries	186
5.9.6	Starting the MAILSRV2 SMTP server.	186
5.9.7	Setting up MAILSRV2 to handle Domino	187
5.9.8	Installing the Domino server on MAILSRV2	187
5.9.9	Setting up your workstation to administer the Domino server.	189
5.9.10	Configuring the Domino server for SMTP mail	189
5.9.11	Creating Lotus Notes mail users	192
Chapter 6.	Single domain with a fanout to multiple systems	193
6.1	Scenario	193
6.1.1	Scenario network configuration	193
6.1.2	Scenario objectives	194
6.1.3	Scenario advantages	194
6.1.4	Scenario limitations	195

6.1.5	Planning considerations	195
6.1.6	Task summary.	197
6.2	Configuring the AS/400 DNS.	197
6.2.1	Task summary.	198
6.2.2	Configuring the AS/400 DNS to handle internal domain.	198
6.2.3	Adding host names to the domain	199
6.2.4	Configuring the MX record for your domain	200
6.2.5	Configuring the internal DNS to forward the queries to the firewall	201
6.3	Configuring IBM Firewall for AS/400 (FW4MAIL).	202
6.3.1	Scenario network configuration	202
6.3.2	Task summary.	203
6.3.3	Installing IBM Firewall for AS/400 (FW4MAIL).	203
6.3.4	Performing basic configuration (FW4MAIL)	204
6.4	Configuring IBM eNetwork Firewall for Windows NT (FW4NT)	208
6.4.1	Scenario network configuration	208
6.4.2	Task summary.	209
6.4.3	Installing IBM eNetwork Firewall for Windows NT (FW4NT)	209
6.4.4	Setting up IBM eNetwork Firewall for Windows NT	210
6.5	Planning the Domino server on AS/400 systems.	221
6.5.1	Planning considerations	221
6.6	Configuring the three Domino servers	224
6.6.1	Task summary.	224
6.6.2	Configuring the Domino server for SMTP mail.	224
6.6.3	Linking the Domino server with the firewall	227
6.7	Linking and trusting the Domino servers together	228
6.7.1	Task summary.	228
6.7.2	Creating domain documents	229
6.7.3	Creating connection documents	231
6.7.4	Cross certifying the Domino servers	235
6.8	Configuring replications	239
6.8.1	Task summary.	239
6.8.2	Giving replication authority to the Domino servers.	240
6.8.3	Setting up replications.	242
6.8.4	Enabling Public Address Book lookup	244
6.9	Creating Lotus Notes mail users	246
Chapter 7.	Problem determination	249
7.1	IBM Firewall for AS/400	249
7.2	IBM eNetwork Firewall for Windows NT	250
7.3	AS/400 e-mail problem determination	251
7.4	OS/400 SMTP and Lotus Domino R5 configured *MSF	251
7.4.1	Outbound or Inbound mail flow on the AS/400 interface	251
7.4.2	Pre-V4R4 Flight Recorders and the V4R4 Flight Recorders	252
7.4.3	Mail flow through the Mail Server Framework (MSF)	252
7.4.4	Tracking mail through SMTP, MSF, and internal AS/400 objects.	252
7.4.5	Monitoring mail using Domino Message Tracking	253
7.5	Lotus Domino using native Domino SMTP on the AS/400 system	253
7.6	Collecting pre-V4R4 SMTP Flight Recorders.	253
7.7	Collecting V4R4 Flight Recorders	255
7.7.1	TRCTCPAPP parameter settings for e-mail on the AS/400 system	255
7.7.2	SMTP inbound connections *SMTPSVR	255
7.7.3	SMTP outbound connections *SMTPCLT	257
7.8	AnyMail/MSF dump snap-in	260

7.9 Dumping Mail Server Framework (MSF)	261
7.10 Taking a communications trace of a line	261
7.10.1 Collecting the line trace	261
7.11 Component Journaling	263
7.11.1 AS/400 Mail Component Journaling Web page	264
7.11.2 Managing journal receivers	264
7.11.3 Description of the major components	264
7.11.4 Journaling considerations	266
7.11.5 Viewing the journal receiver	267
7.11.6 Mail Server journal entries	269
7.12 EDTF	274
7.13 Web site for PTF cover letters and APARS	274
7.14 POP3 Mail	274
7.14.1 Tips on debugging mail on an AS/400 system	274
7.15 Tools for e-mail monitoring with Domino	280
7.15.1 Tracking mail messages	280
7.15.2 How mail tracking works	280
7.15.3 Generating mail usage reports	281
7.15.4 Mail probes	281
7.16 Setting up the Reports database for Domino	283
7.16.1 Security	283
7.17 Controlling the Mail Tracking Collector	283
7.18 Configuring the server for message tracking	284
7.19 Tracking a mail message	285
Chapter 8. Installing a Windows NT Server to support firewalls	289
8.1 Overview	289
8.2 AS/400 planning	289
8.3 Windows NT planning	293
8.4 Disk storage sizing considerations	294
8.5 Hardware and software checklists	296
8.6 Installation worksheets	297
8.6.1 SPD packaging	301
8.6.2 PCI packaging	302
8.6.3 Installation steps	303
8.7 Completing the pre-installation tasks	303
8.8 Starting the Windows NT Server installation from the AS/400 system	305
8.9 Completing the installation from the Windows NT console	310
8.10 Determining the port to Windows NT Server adapter number	316
8.11 Completing the post-installation tasks	318
Appendix A. Implementing other firewall functions	321
A.1 Creating and using a package file	321
A.2 IP address alias on the secure LAN	322
A.3 IP address alias on the non-secure LAN	323
A.4 Preventing spam mail from reaching secure clients	324
A.4.1 Blocking spam by domain name	324
A.4.2 Blocking spam by sender name and domain	325
A.4.3 Blocking spam by source IP address	326
A.5 Nesting firewalls in a network	326
A.5.1 Adding forwarders to the firewall DNS configuration	326
A.5.2 Chaining the HTTP proxy to another server	327

Appendix B. Using virtual IP addresses	329
B.1 What is a virtual IP address?	329
B.2 Configuring virtual IP addresses	329
B.2.1 Task summary	330
B.2.2 Selecting a network address to use as virtual IP addresses	330
B.2.3 Defining the virtual IP addresses on the system	330
B.2.4 Adding the route entries	333
B.2.5 Adding the system names to the DNS	333
B.2.6 Starting the interfaces	333
B.2.7 Testing the connectivity	334
B.3 Virtual IP addresses and e-mail	334
Appendix C. DNS concepts	335
C.1 IBM eNetwork Firewall for Windows NT DNS implementation	335
C.2 Overview	335
C.3 Domain versus zone of authority	337
C.4 Name resolution	339
C.5 Types of name servers	341
C.6 Split DNS concept for firewalls	344
C.7 Primary domain files	344
C.8 Types of records	346
C.9 Round robin and address sorting	347
C.10 For more information	347
Appendix D. Firewall concepts	349
D.1 SMTP relay function	349
D.1.1 Inbound message process	349
D.1.2 Outbound message process	349
D.2 IBM Firewall for AS/400 DNS records created during basic configuration	349
D.3 IBM Firewall for AS/400 advanced DNS configuration	350
D.3.1 Public domain	351
D.3.2 Public name server and IP address	352
D.4 Additional firewall information	352
Appendix E. Special notices	353
Appendix F. Related publications	355
F.1 IBM Redbooks publications	355
F.2 IBM Redbooks collections	355
F.3 Other resources	355
F.4 Referenced Web sites	356
How to get IBM Redbooks	357
IBM Redbooks fax order form	358
Index	359
IBM Redbooks evaluation	365

Figures

1. Network with one domain and subdomains on a single mail server	12
2. Network configuration for multiple domains on a single server	13
3. Network configuration for multiple domains on a single server	14
4. Network configuration for one domain with fanout	15
5. Configuring one domain with subdomains on a single mail server	18
6. Configuring the AS/400 DNS to handle the internal domain: domain.com	22
7. New Primary Domain: domain.com	23
8. Content of Primary Domains after creating domain.com	23
9. Adding the AS/400 host name	24
10. Content of Primary Domains after creating the three subdomains	25
11. Adding an MX record for a subdomain.	25
12. Configuring the internal DNS to forward queries to the firewall	26
13. Adding the IP address of the firewall to the forwarders list	27
14. One domain with subdomains on IBM Firewall for AS/400	28
15. Firewall installation summary page (FW1MAIL).	29
16. Starting the firewall (FW1MAIL)	29
17. Basic firewall configuration summary page for FW1MAIL (Part 1 of 2)	31
18. Basic firewall configuration summary page for FW1MAIL (Part 2 of 2)	32
19. Confirmation that the firewall is configured	33
20. Selection of NAT from the Configuration Menu	34
21. Network Address Translation Settings page	34
22. Insert NAT directive	35
23. Creating a NAT MAP setting	35
24. Displaying NAT Settings	36
25. Starting NAT and IP forwarding from the Status window	36
26. Custom rules inserted prior to the ending defenses.	37
27. One domain with subdomains on IBM eNetwork Firewall for Windows NT	39
28. Starting the firewall wizard	40
29. Firewall wizard welcome screen	41
30. What to Expect firewall wizard	41
31. Important notice firewall wizard	42
32. Network interface selection	42
33. Secure Network configuration	43
34. Domain Name Services	43
35. Secure DNS IP address.	44
36. Non-secure DNS IP addresses	44
37. Secure Mail Proxy	45
38. Add a secure mail server	45
39. Secure Mail Proxy display	46
40. Security policies configuration	46
41. Web Access	47
42. Web Access via Proxy, Socks, or Filtered Only	47
43. Web Access services.	48
44. Telnet Access.	48
45. FTP Access	49
46. Firewall Log	49
47. Alert Log.	50
48. Log Monitor Thresholds	50
49. Default User Setup.	51
50. Setup activation	51

51. Advanced IP Addressing	52
52. Network Address Translation Configuration Administration	53
53. Add NAT Entry	53
54. Activate NAT map settings	54
55. Update NAT configuration.	54
56. Rule Administration	55
57. Add a Rule Template	56
58. Add Service	57
59. Add Service	57
60. Network Object Administration	58
61. Define a Network Object	58
62. Connection Administration	59
63. Add a New Connection	59
64. Control Activity Status of the Connection Rules	60
65. Change SMTP Attributes	62
66. CHGTCPDMN - Search priority *LOCAL	63
67. Associating an IP address with a mail domain	63
68. Firewall configuration on the AS/400 TCP/IP host table	64
69. Change POP server attributes	65
70. TCP/IP default route configuration	66
71. Creating a POP3 account	67
72. Work with directory entries	67
73. Add Directory Entry (Part 1 of 2)	68
74. Add Directory Entry (Part 2 of 2)	68
75. Adding an SMTP user ID and domain.	68
76. Work with Directory Entries.	69
77. Change Directory Entry (Part 1 of 2)	69
78. Changing Directory Entry (Part 2 of 2)	70
79. Adding an SMTP user ID and domain.	70
80. Add TCP/IP Interface	72
81. Configure Domino Server (Part 1 of 4)	73
82. Configure Domino Server (Part 2 of 4)	73
83. Configure Domino Server (Part 3 of 4)	73
84. Configure Domino Server (Part 4 of 4)	74
85. Lotus Notes Client Configuration - Setting up connections.	75
86. Lotus Notes Client Configuration - Connecting to a Domino server	75
87. Lotus Notes Client Configuration - User ID	76
88. Lotus Notes Client Configuration - Connecting to a remote server.	76
89. Lotus Notes Client Configuration - Setting up an Internet mail account	77
90. Lotus Notes Client Configuration - Finish	77
91. Lotus Domino Administrator desktop	78
92. Adding a location.	79
93. Location document - Basics	79
94. Location document - Servers	80
95. Location document - Mail	80
96. Location document - Advanced.	81
97. Selecting your location document	81
98. Server Bookmark	82
99. Favorites window	82
100. Domain document	83
101. Domain document - Basics.	83
102. Domain document - Conversion	84
103. Server document	84

104.Server document - Basics	85
105.Configuration document.	85
106.Configuration document - Router/SMTP	86
107.Registration - Person.	87
108.Certifier ID password.	87
109.Register Person (Part 1 of 2).	88
110.Register Person (Part 2 of 2).	89
111.Scenario network configuration for multiple domains on a single server.	92
112.Configuring the AS/400 DNS to handle the internal domain: domain.com	96
113.New Primary Domain domain.com	97
114.Content of Primary Domains after creating domain.com.	97
115.Adding the AS/400 host name.	98
116.Content of Primary Domains after creating the three domains	99
117.Adding an MX record in a domain	99
118.Configuring the internal DNS to forward queries to the firewall	100
119.Adding the IP address of the firewall to the forwarders list	101
120.Multiple domains on a single mail server with IBM Firewall for AS/400.	102
121.Firewall Installation summary page (FW2MAIL)	103
122.Starting the firewall (FW2MAIL).	103
123.Basic firewall configuration summary page for FW2MAIL (Part 1 of 2).	105
124.Basic firewall configuration summary page for FW2MAIL (Part 2 of 2).	106
125 Confirmation that the firewall is configured	107
126.Mail selection in the Configuration Menu.	107
127.Secure Mail Servers window	108
128.Restarting DNS and Mail from the Status window.	108
129.Multiple domains on a single mail server - NT.	109
130.Starting firewall wizard.	110
131.Welcome screen firewall wizard	111
132.What to Expect firewall wizard.	111
133.Important notice firewall wizard	112
134.Network interface selection	112
135.Secure Network configuration	113
136.Domain Name Services.	113
137.Secure DNS IP address.	114
138.Non-secure DNS IP addresses	114
139.Secure Mail Proxy	115
140.Adding a secure mail server	115
141.Secure Mail Proxy	116
142.Security policies configuration.	116
143.Web Access.	117
144.Web Access via Proxy, Socks, or Filtered Only.	117
145.Web Access services.	118
146.Telnet Access	118
147.FTP Access	119
148.Firewall Log	119
149.Alert Log	120
150.Log Monitor Thresholds.	120
151.Default User setup.	121
152.Setup Activation.	121
153.Change SMTP Attributes.	122
154.CHGTCPDMN - Search priority *LOCAL.	123
155.Associating an IP address with the mail domain	123
156.Firewall configuration on the AS/400 TCP/IP host table	124

157.Change POP Server Attributes	125
158.Creating a POP3 account.	126
159.Work with Directory Entries	127
160.Add Directory Entry (Part 1 of 2)	127
161.Add Directory Entry (Part 2 of 2)	127
162.Adding an SMTP user ID and domain	128
163.Work with Directory Entries	128
164.Change Directory Entry (Part 1 of 2)	129
165.Changing Directory Entry (Part 2 of 2)	129
166.Add SMTP user ID and domain	130
167.Domain document	131
168.Domain document - Basics.	132
169.Domain document - Conversion	132
170.Server document	133
171.Server document - Basics	133
172.Configuration document	134
173.Configuration document - Router/SMTP	134
174.Registration - Person	135
175.Certifier ID password	135
176.Register Person (Part 1 of 2)	136
177.Register Person (Part 2 of 2)	137
178.Scenario network configuration for multiple domains on a single server	140
179.Configuring the AS/400 DNS to handle the internal domain: domain.com	144
180.New Primary Domain domain.com	145
181.Content of Primary Domains after creating domain.com	145
182.Content of Primary Domains after creating the three domains.	146
183.Adding the AS/400 host name	146
184.Adding an MX record in a domain	147
185.Configuring the internal DNS to forward queries to the firewall	148
186.Adding the IP address of the firewall to the forwarders list.	148
187.Multiple domains on multiple mail servers with IBM Firewall for AS/400	149
188.Firewall Installation summary page (FW3MAIL)	150
189.Starting the firewall (FW3MAIL)	150
190.Basic firewall configuration summary page for FW3MAIL (Part 1 of 2)	152
191.Basic firewall configuration summary page for FW3MAIL (Part 2 of 2)	153
192 Confirmation that the firewall is configured.	154
193.Multiple mail servers with IBM eNetwork Firewall for Windows NT	154
194.Starting firewall wizard	155
195.Welcome screen firewall wizard	156
196.What to Expect firewall wizard	156
197.Important notice firewall wizard	157
198.Network interface selection	157
199.Secure Network configuration	158
200.Domain Name Services	158
201.Secure DNS IP address	159
202.Non-secure DNS IP addresses	159
203.Secure Mail Proxy	160
204.Adding a secure mail server	160
205.Secure Mail Proxy	161
206.Security policies configuration	161
207.Web Access	162
208.Web Access via Proxy, Socks, or Filtered Option	162
209.Web Access services	163

210.Telnet Access	163
211.FTP Access	164
212.Firewall Log	164
213.Alert Log	165
214.Log Monitor Thresholds.	165
215.Default User Setup	166
216.Setup Activation.	166
217.Change SMTP Attributes.	167
218.CHGTCPDMN - Search Priority *LOCAL	168
219.Associating an IP address with the mail domain	168
220.Firewall configuration on AS/400 TCP/IP host table	169
221.Change POP Server Attributes	170
222.Creating a POP3 account	171
223.Work with Directory Entries	171
224.Add Directory Entry (Part 1 of 2)	172
225.Add Directory Entry (Part 2 of 2)	172
226.Adding an SMTP user ID and domain.	172
227.Work with Directory Entries	173
228.Change Directory Entry (Part 1 of 2)	173
229.Changing Directory Entry (Part 2 of 2).	174
230.Adding an SMTP user ID and domain.	174
231.Domain document	177
232.Domain document - Basics	178
233.Domain document - Conversions	178
234.Server document	179
235.Server document - Basics	179
236.Configuration document.	180
237.Configuration document - Router/SMTP	180
238.Registration - Person.	181
239.Certifier ID password.	181
240.Register Person (Part 1 of 2).	182
241.Register Person (Part 2 of 2).	183
242.Change SMTP Attributes.	184
243.CHGTCPDMN - Search Priority *LOCAL	185
244.Associating an IP address with a mail domain	185
245.Firewall configuration on the AS/400 TCP/IP host table	186
246.Add TCP/IP Interface.	187
247.Configure Domino Server (Part 1 of 4)	188
248.Configure Domino Server (Part 2 of 4)	188
249.Configure Domino Server (Part 3 of 4)	189
250.Configure Domino Server (Part 4 of 4)	189
251.Domain document (MTAGlobal)	190
252.Domain document - Basics (MTAGlobal)	190
253.Domain document - Conversion (MTAGlobal).	191
254.Server document	191
255.Server document - Basics	192
256.Server document - MTAs.	192
257.Scenario network configuration for one domain with fanout	194
258.Configuring the AS/400 DNS to handle the internal domain domain.com.	198
259.New Primary Domain domain.com	199
260.Contents of Primary Domains after creating domain.com	199
261.Adding the AS/400 host name.	200
262.Adding an MX record in a domain	200

263.	Configuring the internal DNS to forward queries to the firewall	201
264.	Adding the IP address of the firewall to the forwarders list.	202
265.	Single domain with fanout - IBM Firewall for AS/400	203
266.	Firewall Installation summary page (FW4MAIL)	204
267.	Starting the firewall (FW4MAIL)	204
268.	Basic firewall configuration summary page for FW4MAIL (Part 1 of 2)	206
269.	Basic firewall configuration summary page for FW4MAIL (Part 2 of 2)	207
270.	Confirmation that the firewall is configured.	208
271.	Single domain with fanout - IBM eNetwork Firewall for Windows NT	209
272.	Starting firewall wizard	210
273.	Welcome screen firewall wizard	210
274.	What to Expect firewall wizard	211
275.	Important notice firewall wizard	211
276.	Network interface selection	212
277.	Secure network configuration	212
278.	Domain Name Services	213
279.	Secure DNS IP address	213
280.	Non-Secure DNS IP addresses	214
281.	Secure Mail Proxy	214
282.	Adding a secure mail server	215
283.	Secure Mail Proxy	215
284.	Security policies configuration	216
285.	Web Access	216
286.	Web Access via Proxy, Socks, or Filtered Only	217
287.	Web Access services	217
288.	Telnet Access	218
289.	FTP Access	218
290.	Firewall Log	219
291.	Alert Log	219
292.	Log Monitor Thresholds	220
293.	Default User setup	220
294.	Setup Activation	221
295.	Mail flow between the Domino servers and the firewall	222
296.	Domain document	225
297.	Domain document - Basics.	225
298.	Domain document - Conversion	226
299.	Server document	226
300.	Server document - Basics	227
301.	Configuration document	227
302.	Configuration document - Router / SMTP	228
303.	Domain document	229
304.	Domain document - Basics.	229
305.	Domain document - Basics.	230
306.	Domain documents.	230
307.	New connection document	231
308.	Connection document - Basics	232
309.	Connection document - Replication/Routing	232
310.	Connection document - Schedule	233
311.	Connection document - Basics	233
312.	Connection document - Replication/Routing	234
313.	Connection document - Schedule	235
314.	Connection documents.	235
315.	Cross certify - Certification pull-down menu	236

316.Choose Certifier ID	236
317.Entering a certifier password	237
318.Choose ID to be Cross-Certified	237
319.Issue Cross Certificate.	237
320.Cross certifying another organization	238
321.Choose ID to be Cross-Certified	238
322.Issue Cross Certificate.	238
323.Cross certifying another organization	239
324.Notes Cross Certificates	239
325.Selecting the group OtherDomainServers.	240
326.Group OtherDomainServer - Basics	240
327.Server document	241
328.Server document - Security	241
329.Replication	242
330.Replication - Choose Database.	243
331.Replication - New Replica "mailsrv2's Address Book".	243
332.Replication - Choose Database.	243
333.Replication - New Replica "mailsrv3's Address Book".	244
334.Replication - Result	244
335.Work with Domino Servers	245
336.Edit Notes.ini (Part 1 of 2)	245
337.Edit Notes.ini (Part 2 of 2)	246
338.Registration - Person.	246
339.Certifier ID password.	247
340.Register Person (Part 1 of 2)	247
341.Register Person (Part 2 of 2)	248
342.Trace TCP/IP Application (TRCTCPAPP) - SMTPSVR.	256
343.Trace TCP/IP Application (TRCTCPAPP) - SMTPCLT.	258
344.Starting the communications trace	262
345.Format Trace Data.	263
346.AS/400 Mail Components	265
347.Locating a POP3 mailbox on the AS/400 system	279
348.Mail distributions in the JONEST2 POP3 mailbox on the AS/400 system.	280
349.Graphical user interface for Domino Message Tracking	286
350.Integrated Netfinity Server SPD packaging	302
351.Integrated Netfinity Server PCI packaging.	303
352.INSWNTSVR display (Part 1 of 4)	307
353.INSWNTSVR display (Part 2 of 4)	308
354.INSWNTSVR display (Part 3 of 4)	308
355.INSWNTSVR display (Part 4 of 4)	309
356.TCP/IP settings for a Token-Ring PCI adapter	312
357.Enter TCP/IP address for the virtual LAN adapter.	313
358.TCP/IP settings - Routing	314
359.Setting the Windows NT Time Zone	315
360.Contents of the e:\mptn\bin\setup.cmd file	322
361.Package file to add an additional IP address to the secure port	323
362.Package file to remove an additional IP address from the secure port	323
363.Package file to add an additional IP address to the non-secure port	324
364.Package file to block e-mail based on a domain name	325
365.Package file to block e-mail based on a fully-qualified name	325
366.Package file to block e-mail based on fully-qualified name	326
367.Package file to add forwards to the firewall DNS.	327
368.Package file to remove forwards from the firewall DNS	327

369.Package file to add HTTP proxy chaining to the HTTP proxy	327
370.Package file to remove HTTP proxy chaining from the HTTP proxy	328
371.Sample network using virtual IP addresses	329
372.Adding a virtual IP address.	331
373.Specifying the IP address information	331
374.New TCP/IP Interface Summary display	332
375.TCP/IP interfaces with all addresses added.	333
376.DNS name space	336
377.Hosts with the same names in different domains	337
378.Domain, subdomain, delegation, and zone of authority	339
379.Name resolution example.	340
380.Basic firewall configuration summary	350
381.Advanced DNS configuration	351
382.Advanced DNS configuration - Public domain	352
383.Public name server.	352

Tables

1. V4R4 abbreviations and the corresponding pre-V4R4 text	4
2. Evaluation of current e-mail environment.	9
3. Future e-mail requirements	10
4. Domain names, host names, and IP addresses	19
5. Secure mail server name - DNS MX values.	20
6. Domain name and secure mail server name - Firewall values	20
7. User values for domain name, host name, and IP address	20
8. User values for secure mail server name - DNS MX values	21
9. User values for domain name and secure mail server name - Firewall	21
10. Domain names, host names, and IP addresses	93
11. Secure mail server name - DNS MX values.	94
12. Domain name and secure mail server name - Firewall values	94
13. User values for domain name, host name, and IP address	94
14. User values for secure mail server name - DNS MX values	95
15. User values for domain name and secure mail server name - Firewall	95
16. Domain names, host names, and IP addresses	141
17. Secure mail server name - DNS MX values.	142
18. Domain name and secure mail server name - Firewall values	142
19. User values for domain name, host name and IP address	143
20. User values for secure mail server name - DNS MX values	143
21. User values for domain name and secure mail server name - Firewall	143
22. Configuration values for DOM400 and DOMINO2.	176
23. User configuration values.	176
24. Domain names, host names, and IP addresses	195
25. Secure mail server name - DNS MX values.	196
26. Domain name and secure mail server name - firewall values	196
27. User values for domain name, host name, and IP address	196
28. User values for the secure mail server name - DNS MX values	197
29. User values for the domain name and secure mail server name - Firewall	197
30. Configuration values for DOM400, DOMINO2, and DOMINO3	223
31. Configuration values for user systems.	223
32. Spooled files generated by the SMTP Flight Recorder	254
33. Parameters for TRCTCPAPP APP(*SMTPSVR)	256
34. Parameters for TRCTCPAPP APP(*SMTPCLT)	258
35. Function identifiers.	267
36. Second character of SubType/code.	268
37. Journal entry abbreviations	269
38. Mail Server journal entries	269
39. SMTP client	270
40. SMTP Serve	271
41. Bridge server	272
42. Additional MSF and POP journal points.	273
43. Additional MSF and POP journal points.	273
44. Journaling points not in SMTP or the framework	274
45. Domino Message Tracking - Delivery status	281
46. Fields to complete on the Basics tab for a mail probe	282
47. Fields to complete on the Probe tab for a mail probe	282
48. Fields to complete on the Other tab for a mail probe	282
49. Values for creating the Reports database	283
50. Tasks for managing mail tracking	284

51. Server configuration fields for message tracking	285
52. Message tracking options	287
53. Hardware checklist	296
54. Software checklist	296
55. Installation worksheet to support firewalls on the Integrated Netfinity Server .	297
56. Interface worksheet	301
57. Installation worksheet used in our Integrated Netfinity Server configuration .	306
58. Interface worksheet used in our Integrated Netfinity Server configuration . .	307
59. Port number to adapter number mapping	316
60. Sample port number to adapter number mapping	318

Preface

Learn how to plan, install, tailor, configure, and troubleshoot a firewall installation that supports e-mail. This redbook provides sample scenarios that demonstrate several ways to handle multiple SMTP mail domains behind a firewall. We use two firewall products in these samples: IBM Firewall for AS/400 and IBM eNetwork Firewall for Windows NT V3. This redbook targets the needs of analysts, consultants, and support people that will design, install, and configure the e-mail environment.

For the e-mail functions, this redbook shows both base AS/400 Mail Server Framework (MSF) SMTP and POP server support, as well as using Lotus Domino R4.66 and Lotus Domino R5.03. The samples do not specifically include IBM SecureWay Firewall V4.1 for Windows NT announced September 28, 1999. However, the demonstrated techniques can be applied using the new product as well as firewalls from other vendors. The configuration of other firewall functions are not specifically covered in this book. You may need to refer to other firewall documentation for additional configuration information.

This redbook also covers basic Domino setup to support mail environments. Some knowledge of the AS/400 platform and TCP/IP is assumed.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Rochester Center.

Fant Steele is an Advisory ITSO Specialist for AS/400 in the International Technical Support Organization, Rochester Center. He writes extensively and teaches IBM classes worldwide on many areas of AS/400 communications technologies and e-business. He spent eight years as an instructor and developer for the AS/400 communications and programming curriculum of IBM Education and Training. Prior to joining IBM in 1989, he worked on S/36 to AS/400 code conversion, VM/MVS systems programming, and applications programming for the manufacturing industry.

Marc Jenni is an Advisory IT Specialist in Le Service Informatique de La Caisse de Compensation du Jura, which is an IBM Business Partner in Switzerland. He has worked with IBM products for six years, including two years of experience in the AS/400 field. His areas of expertise include IT security consulting, Internet services on AS/400, Firewall for AS/400, TCP/IP, and AS/400 monitoring.

Thanks to the following people for their invaluable contributions to this project:

Justine Middleton
Marcela Adan
International Technical Support Organization, Rochester Center

Kevin Hubbard
Daryl Spartz
Boyd Gerber
George Romano

Walter Scanlan
IBM Rochester

Francis A. Pflug
Susan Hall
IBM Endicott

David Lee
IBM Australia

Birgit Roehm
IBM Germany

Katina Chan
IBM Hong Kong

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Please send us your comments about this or other Redbooks in one of the following ways:

- Fax the evaluation form found in “IBM Redbooks evaluation” on page 365 to the fax number shown on the form.
- Use the online evaluation form found at <http://www.redbooks.ibm.com/>
- Send your comments in an Internet note to redbook@us.ibm.com

Chapter 1. What is new in the IBM Firewall for AS/400 V4R4

This chapter provides an overview of the enhancements to IBM Firewall for AS/400 in V4R4. It also provides a summary of the hardware and software requirements and briefly reviews the functions available in IBM Firewall for AS/400 since its announcement in V4R1.

1.1 Hardware and software requirements

The following are the hardware and software requirements for IBM Firewall for AS/400 V4R4:

- OS/400 V4R4 (5769-SS1)
- One Integrated PC Server (IPCS) or Integrated Netfinity Server with *two* LAN adapters and 64 MB of memory (no more than 512 MB)
- Integration Services for FSIOP (5769-SA2)
- IBM Firewall for AS/400 V4R4 (5769-FW1)
- IBM HTTP Server for AS/400 (5769-DG1): This product is needed for firewall installation
- Domain Name System (DNS) (5769-SS1 option 31)
- OS/400 TCP/IP Connectivity Utilities (5769-TC1)
- IBM Cryptographic Access Provider (5769-AC1, AC2, AC3): One of these products is needed for Virtual Private Networks (VPN) support
- DB2 Query Manager and SQL Development Kit for AS/400 (5769-ST1): This product is needed for the log analysis tool and management
- One administrator client with a browser that supports HTML frame and JavaScript (Netscape Navigator 3.0 or later, or Internet Explorer 4.0 or later)

Important

You *must* install IBM Cryptographic Access Provider (5769-AC1, AC2, AC3) *before* you vary on IBM Firewall for AS/400 to use the VPN support.

If the firewall is varied on before the appropriate 5769-ACx licensed program product is installed, you must restore IBM Firewall for AS/400 (use the Restore Licensed Program (RSTLICPGM) command). If necessary, reload and reapply the firewall PTFs. No firewall configuration changes are required. The existing firewall configuration is preserved.

1.2 IBM Firewall for AS/400 positioning

Before deciding on a firewall product, document the current network environment and desired network environment. Complete the following tasks:

1. Describe why an Internet connection is necessary and what risk level is acceptable to have one.

2. Identify the access requirements precisely. Include the services that should be provided to internal users and what services are to be made available to the Internet.
3. Define who is to be involved during the firewall selection, installation, and maintenance phases. You also need to define the approvals necessary to make changes.

This document may be the beginning of a network security policy if you do not already have one.

Until you define your requirements, you should not make a decision about which firewall product to use. IBM Firewall for AS/400 is an entry-level firewall product that is designed to meet the needs of most small-to-medium sized businesses. However, it is not the right choice for everyone.

IBM Firewall for AS/400 is the right choice if:

- Your organization is a small-to-medium sized enterprise or it is within a large enterprise where the AS/400 system is the predominant server.
- Your connection to the ISP is T1 or less.
- Your internal users are allowed to browse the Internet, download files, exchange e-mail, and signon to remote systems.
- Your Internet users are allowed to access the AS/400 system behind the firewall with HTTP or HTTPS.

Consider another firewall product if any of the following scenarios are true:

- Your organization is a large enterprise or has high growth potential.
- Your connection to ISP is greater than T1.
- You have hundreds of internal users.
- You have high e-mail volume with large attachments.
- You require advanced authentication devices such as SecurID.
- You require multiple firewalls with a single shared console.

If IBM Firewall for AS/400 does not meet your needs, we encourage you to look at other products such as IBM SecureWay Firewall V4.1 for Windows NT or AIX.

1.3 IBM Firewall for AS/400 components

IBM Firewall for AS/400 was announced in September of 1997. The features and functions available in IBM Firewall for AS/400 *before* V4R4 are:

- Internet Protocol (IP) packet filtering for TCP, UDP, and ICMP packets
- Proxy server for HTTP, HTTPS, FTP (passive and active), Gopher, and Wide Area Information System (WAIS) (these proxy servers are available *only* through a Web browser)
- Proxy server for TELNET (not through Web browser)
- SOCKS server (SOCKS 4 and SOCKS 5)
- Mail relay service
- Split Domain Name Services (DNS)
- Logging services

- Monitoring services
- Network Address Translation (NAT)
- Virtual Private Networks (VPN)
- Basic configuration (firewall configuration wizard):
 - Secure mail server
 - Web servers behind the firewall (bypassing SOCKS and Proxy servers and requiring registered IP address and IP forwarding enabled)
 - Web servers behind the firewall using NAT added at V4R3
 - NAT configuration for internal clients
 - Proxy or SOCKS server, for access from the secure network to the Internet for the following services:
 - HTTP
 - HTTPS
 - FTP (Passive or active)
 - TELNET
 - Gopher
 - WAIS
 - SOCKS server, for access from the secure network to the Internet for the following services:
 - Internet relay chat (IRC)
 - Real audio
 - Lotus Notes
 - LDAP
 - Secure LDAP
 - Server Mapper (CA/400)
 - DRDA
 - POP3 Mail

1.4 IBM Firewall for AS/400 V4R4 enhancements

The enhancements to IBM Firewall for AS/400 in V4R4 are:

- Multiple domain support
- Multiple mail servers
- Changes to packet filter log messages
- Improved operation of the start button
- DNS name explanation for V4R4
- Improved usability due to changes in the NAT MAP setting syntax
- New IPCS hardware
- New name for the IPCS and FSIOIP cards

1.4.1 Multiple domain support

Multiple secure or non-secure domains can be specified during Basic configuration, or by using the DNS link on the Configuration menu or directly using the DNS URL (<http://firewall.my.com:2001/cgi-bin/db2www/fsdns.mac/main>). Also, the DNS link has been improved so that it can now be used after the DNS URL has been used. In previous releases, if the DNS link was used to make any changes, the DNS configuration was completely redone from scratch

so that any previous modifications made with the DNS URL would be lost. This is no longer the case with V4R4. The DNS link and the DNS URL can both be used without losing any configuration data.

1.4.2 Multiple mail servers

In addition to multiple domain support, the firewall's mail relay can be set up to relay mail to multiple secure mail servers. For example, external mail addressed to multiple non-secure (public) domains may be relayed to multiple secure (internal) domains and their associated mail servers. You set up the mapping of domains to secure mail servers in Basic configuration or by using the Mail link on the Configuration menu. The firewall supports a maximum of 10 mail domains.

1.4.3 Changes to packet filter log messages

Eight packet filter log messages, ICA1038 through ICA1045, have been shortened. Prior to V4R4, these messages typically were about 290 characters wide. In V4R4, these messages were shortened to about 170 characters by using abbreviations.

As an example, prior to V4R4, a typical ICA1039 message looked like this:

```
17:00:09 ICA1039i: Permitted packet in. Rule: 5 Source addr: 10.10.11.6
Destination addr: 10.10.10.10 Protocol: tcp Source port: 1114 Destination port:
23 Routing: route Interface: non-secure Adapter: 100.53.29.15 Fragment: n VPN:
2 Encryption: D Size: 40.
```

In V4R4, the same message looks like this:

```
17:00:09 ICA1039i: PIN R: 5 S: 10.10.11.6 D: 10.10.10.10 SP: 1114 DP: 23 RT:
route I: non-secure PR: tcp A: 100.53.29.15 F: n V: 2 E: D SZ: 40.
```

Table 1 shows the V4R4 abbreviations and the corresponding pre-V4R4 text.

Table 1. V4R4 abbreviations and the corresponding pre-V4R4 text

V4R4 abbreviation	Pre-V4R4 text
PIN	Permitted packet in
POUT	Permitted packet out
DIN	Denied packet in
DOUT	Denied packet out
R	Rule
S	Source addr
D	Destination addr
SP	Source port
DP	Destination port
RT	Routing
I	Interface
A	Adapter
F	Fragment

V4R4 abbreviation	Pre-V4R4 text
V	VPN
E	Encryption
SZ	Size
ICMPT	ICMP Type
ICMPC	ICMP code

1.4.4 Improved operation of the Start button

The Start button is improved so that it says the firewall is started only after the IPCS has varied on and the firewall applications have actually started. In previous releases, after clicking on the Start button, it would immediately say that the firewall had started. It will now report that the firewall is started at the end of the startup process, rather than at the beginning of the process.

To allow this, two new "permit" filter rules are needed. The rules are automatically generated by doing Basic configuration in V4R4, or they can be manually added to the filter rules. If you manually add them, we suggest that they be placed at the top of the filter settings with the other port 2001 rules.

Customers that upgrade from a previous release of the firewall to V4R4, and do not run the Basic configuration, need to manually add these two rules. If Basic configuration is run, the rules are automatically added.

```

permit x.x.x.x 255.255.255.255 a.a.a.a 255.255.255.255 tcp ge 1024 eq 2001
secure local inbound f=y l=n t=0 # Permit *INTERNAL traffic
permit a.a.a.a 255.255.255.255 x.x.x.x 255.255.255.255 tcp/ack eq 2001 ge 1024
secure local outbound f=y l=n t=0 # Permit *INTERNAL traffic

```

Here, x.x.x.x is the *INTERNAL AS/400 IP address, and a.a.a.a is the *INTERNAL firewall IP address.

1.4.5 DNS name explanation for V4R4

If you configured your firewall using Basic configuration prior to V4R4, you may have noticed that the name of the Public Name Server (sometimes referred to as the DNS) was "externaldns." followed by the IP address of the name server. For example, if the IP address of the public name server was 1.1.1.1, then the name was assumed to be "externaldns.1.1.1.1". This can be seen in V4R4 by clicking on the DNS link on the Configuration menu.

Leaving the name as "externaldns." followed by the IP address is okay. However, if you wish, you can use the DNS link in V4R4 to change the name. You can change the name to be what the Public Name Server is, for example, "nameserver.isp.com".

1.4.6 Improved usability due to changes in the NAT MAP setting syntax

An example of an old NAT MAP setting is shown here:

```

action(MAP) from(10.10.11.89) port(0) to(100.2.5.5) port(0)

```

Starting in V4R4, the same NAT MAP setting is:

```
action(MAP) privateAddress(10.10.11.89) privatePort(0)
publicAddress(100.2.5.5) publicPort(0)
```

1.4.7 Basic FastPath

You can still run a basic configuration, or, if you are a firewall administrator, you can now use *Basic FastPath*. This enables direct access to the Review Configuration window, eliminating the need to navigate through all the windows for making the basic configuration of the firewall.

1.4.8 New IPCS hardware

To run the firewall product on the 333 MHz IPCS hardware (announced in February of 1999), you must *not* exceed a maximum of 512 MB of memory on the IPCS card.

1.4.9 New name for the IPCS and FSIOP cards

In addition to the File Server I/O Processor (FSIOP) and the Integrated PC Server (IPCS), you will also see references to the new cards named Integrated Netfinity Server. These cards provide faster processors and can also be used to support IBM Firewall for AS/400 code as well as IBM eNetwork Firewall for Windows NT. IBM Firewall for AS/400 is supported by all cards that are supported by V4R4 of the OS/400 operating system.

1.5 Upgrading IBM Firewall for AS/400 to V4R4

If your company is using IBM Firewall for AS/400 V4R1, V4R2 or V4R3, you can upgrade to V4R4 by completing the following steps:

1. Install the version of IBM Cryptographic Access Provider (5769-AC1, AC2, AC3) available in your country.
2. Install IBM Firewall for AS/400 V4R4.
3. Apply the latest PTFs.
4. Vary on (start) the firewall.

You can now configure a new firewall, or add multiple domains, to an existing configuration.

The order in which you install the licensed program products is *very* important. If you did not install IBM Cryptographic Access Provider *before* installing IBM Firewall for AS/400, you must save 5769-FW1 (use the Save Licensed Program (SAVLICPGM) command), install (5769-AC1, AC2, AC3), and re-install 5769-FW1 (RSTLICPGM).

If you are upgrading from 5769-AC1 to 5769-AC2, you must also re-install 5769-FW1 and its PTFs.

1.6 What has changed since IBM Firewall for AS/400 V4R1

The following list is a quick reference of changes since the first release of IBM Firewall for AS/400 (V4R1). Some of these changes were introduced in V4R2 and V4R3.

- The Internet Protocol Filter (IPFILT) command is no longer available. It is replaced by the Internet Configuration (INETCFG) command. For examples on how to use this command, refer to *IBM Firewall for AS/400 Administrator's Guide*, SC41-5419. This publication is available in soft copy only on the Web at: <http://publib.boulder.ibm.com/html/as400/infocenter.html>
- If the firewall secure port and the secure clients are in different subnets, you no longer need to add the internal route destinations in the firewall Network Server Description (NWS). The *Define the route to the secure clients inside of your firewall* page in the firewall installation allows you to specify the internal route destinations.
- You no longer need to add the secure mail server to the firewall DNS using the firewall Advanced Domain Name Settings to circumvent the problem of not having an internal DNS server. Starting with OS/400 V4R2, the AS/400 system can run a DNS server (OS/400 option 31 must be installed). Therefore, we strongly recommend that you configure an internal DNS server using the OS/400 DNS support. Refer to *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147, for information about configuring OS/400 DNS and IBM Firewall for AS/400. After installing and configuring the internal DNS server, change the NWS description or the value found in option 12 of the Configure TCP (CFGTCP) command to point to the IP address of the internal DNS server.
- If you want to run a public server behind the firewall in the AS/400 system that houses it, you no longer need to change the AS/400 system and firewall *INTERNAL IP addresses from the default reserved address of 192.168.x.x to a registered IP address. The address assigned by the firewall installation program can be used in combination with NAT. You can also configure NAT to use the firewall non-secure port IP address as the public IP address, which does not require additional registered IP addresses. Refer to the redbook *IBM Firewall for AS/400 V4R3: VPN and NAT Support*, SG24-5376.
- If you want to run a public HTTP or HTTPS server behind the firewall, you no longer need to manually configure filters or enable IP forwarding. There are new options in Basic configuration that automate this process. Refer to the redbook *IBM Firewall for AS/400 V4R3: VPN and NAT Support*, SG24-5376.
- If you want to enable your internal users to access Real Audio, you no longer need to change the secure client configuration to use a registered IP address. Use NAT to dynamically assign a registered IP address from a pool to secure clients. Refer to the redbook *IBM Firewall for AS/400 V4R3: VPN and NAT Support*, SG24-5376.
- If you want to enable your internal users to access Lotus Notes, LDAP, Client Access/400, DRDA, POP3, and NNTP servers on the Internet, you no longer need to manually configure the corresponding firewall filter rules. You can specify these services in Basic configuration.
- NAT has been implemented. Network address translation translates secure IP addresses to temporary, publicly registered, addresses from the address pool to communicate with the outside world. The mapping can also be based on a

registered IP address and port number. IBM Firewall for AS/400 V4R3 provides network address translation for any TCP or UDP application, without requiring changes in the data transferred. For more information on IBM Firewall for AS/400 NAT support, refer to the redbook *IBM Firewall for AS/400 V4R3: VPN and NAT Support*, SG24-5376.

- VPN has been implemented. VPNs securely carry information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network. Internet Service Providers (ISPs) offer cost-effective access to the Internet (using direct lines or local telephone numbers), which enables companies to eliminate their current, expensive leased lines, long-distance calls, and toll-free telephone numbers. For more information on IBM Firewall for AS/400 VPN support and implementation examples, refer to the redbook *IBM Firewall for AS/400 V4R3: VPN and NAT Support*, SG24-5376.
- If you want to quickly run basic configuration, or, if you are a firewall administrator, you can use the *Basic FastPath* menu option of the firewall administration. This enables direct access to the Review Configuration window, eliminating the need to navigate through all the windows for making the basic configuration of the firewall.

Chapter 2. Planning your mail environment

One of the most important steps in setting up your e-mail environment is evaluating your current configuration and planning for the future. This chapter helps you in these areas.

2.1 Evaluating your current e-mail environment

The first step in planning your installation is to determine how your e-mail is currently being handled. Use Table 2 to help you collect information about your environment.

Table 2. Evaluation of current e-mail environment

	Question	Answer
1	Do we currently have e-mail implemented? If the answer is "no," skip to 2.2, "Making your plan" on page 10.	
2	Is our e-mail only used for communicating within our company?	
3	Does our e-mail support sending mail to the rest of the world?	
4	Does our e-mail support receiving mail from the rest of the world?	
5	Is our e-mail provided by a third-party e-mail service or Internet Service Provider?	
6	How many e-mail servers do we have in the company?	
7	Are our current SMTP mail domains registered?	
8	What are our current SMTP mail domains?	
9	What are our current mail server software products (OV/400, Domino, OS/400 POP Server, Domino POP Server)? Include the version and release information about each product.	
10	Do we have applications that send e-mail using the Mail Server Framework (MSF) APIs (for example SendMail)?	
11	Are we using the Net.Data function DTW_SendMail to send e-mail?	
12	Do we have a DNS server in our secure network?	
13	Do we have a DNS server in our external network?	
14	Does our ISP provide our external DNS server support for our domains?	

2.2 Making your plan

The second step in planning your installation is to determine your future e-mail requirements. Use Table 3 to help you collect information about your requirements. One assumption is that you are planning to exchange e-mail with the outside world.

Table 3. Future e-mail requirements

	Question	Answer
15	How many e-mail users do we expect to have?	
16	Are we putting all our users in a single SMTP domain?	
17	Do we want different SMTP mail domains for different departments or divisions?	
18	Are our SMTP mail domains registered?	
19	What are our SMTP mail domains?	
20	What mail server software products are we going to use (OV/400, Domino, OS/400 POP Server, Domino POP Server)? Include the version and release information about each product.	
21	Do our users need to access their e-mail from the Internet?	
22	Do we have applications that send e-mail using the Mail Server Framework (MSF) APIs (for example, SendMail)?	
23	Are we using the Net.Data function DTW_SendMail to send e-mail?	
24	Do we have a DNS server in our secure network?	
25	Do we have a DNS server in our external network?	
26	Does our ISP provide our external DNS server support for our domains?	

On the AS/400 system there are three methods to handle the receiving of SMTP mail. They are:

- **Method 1:** OS/400 Mail Server Framework (MSF) listens on the SMTP port (25) and passes the mail to the correct mail application.
- **Method 2:** Domino R5 listens on the SMTP port (25) and passes the mail to the mail processing function of Domino.
- **Method 3:** OS/400 MSF and Domino R5 listen on the SMTP port (25) but at different addresses.

First, you must decide which method you are going to use.

If you answered *yes* to question 10, 11, 22, or 23, you must use Mail Server Framework (MSF) on the systems supporting these applications. If you listed OV/400 or POP server on the AS/400 system in question 9 or 20, you must use MSF. If you are using the SNADS to TCP/IP bridge support, you must use MSF. This is method 1.

If you plan to use Domino and Notes as your only mail solution, you should use method 2.

If the users requiring MSF support are in a different SMTP domain from the users that are going to use Domino support, you may consider using method 3.

If you do not need to exchange e-mail with the rest of the world, you must make sure e-mail support is not configured on your firewall and that the firewall has filter rules in place to block inbound mail.

If your e-mail support is currently provided by an outside vendor, you must determine who owns the domain name and what is involved in moving the domain to your in-house systems.

If you currently have a DNS server in your internal network, you need to verify that it is configured correctly and that it will support your e-mail configuration.

If you do not have an external DNS server and you are going to use IBM eNetwork Firewall for Windows NT, you must either set up an external DNS server or contract with your ISP to provide the DNS service for your external systems and domains.

If your current mail domains are not registered, you should register them immediately. If they are not available, you may have additional changes required in any existing mail configurations because you do not own the mail domain name you are using.

2.3 Scenarios documented in this book

Use the answers in Table 2 on page 9 and Table 3 on page 10 to match your requirements to the samples provided in this book. While there may not be an exact match, you should be able to find a sample that is close to your requirements.

In the following sections, we present an overview of the upcoming scenarios.

2.3.1 One domain with subdomains on a single system

Chapter 3, “One domain with subdomains on a single system” on page 17, presents the procedures for firewall configurations that support a mail environment composed of one domain with multiple subdomains. All subdomains are processed by the same AS/400 system. Figure 1 on page 12 illustrates a logical view of the network configuration used in this scenario.

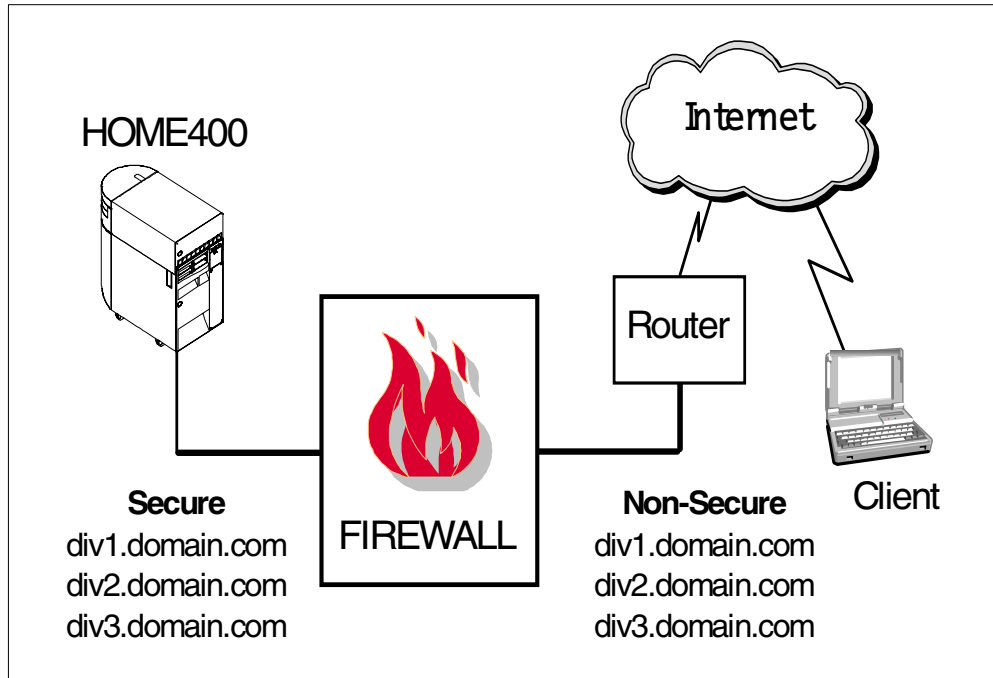


Figure 1. Network with one domain and subdomains on a single mail server

The public mail domains and the private mail domains are the same.

The internal DNS can be on any AS/400 system on the network. In our scenario, the AS/400 system named HOME400 provides this function.

The firewall filters are open to allow POP3 clients and Domino clients on the Internet to access the internal mail server. Network Address Translation (NAT) is used to map the secure address of the mail server to a public address.

2.3.2 Multiple domains on a single system

Chapter 4, "Multiple domains on a single system" on page 91, presents the firewall configurations that support a mail environment composed of multiple domains. All domains are processed by the same mail server. The public mail domains and the private mail domains are the same. Figure 2 on page 13 illustrates a logical view of the network configuration used in this scenario. The internal DNS can be on any AS/400 system on the network. In our scenario, the AS/400 HOME400 provides this function.

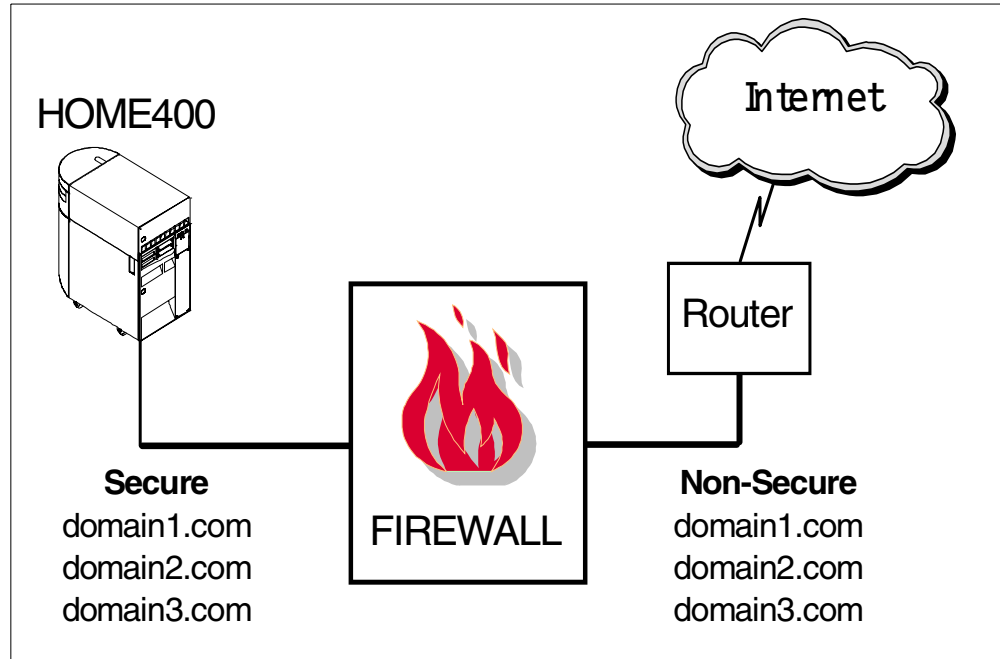


Figure 2. Network configuration for multiple domains on a single server

2.3.3 Multiple domains on multiple systems

Chapter 5, “Multiple domains on multiple systems” on page 139, presents the procedures for firewall configurations that support a mail environment composed of multiple domains. Each domain is processed by one mail server. Figure 3 on page 14 illustrates a logical view of the network configuration used in this scenario.

In this scenario, we present a company that has multiple AS/400 systems. Each of these systems has its own AS/400 system with its own mail domain.

The mail servers are configured as follows:

- SMTP with POP3 server on the AS/400 MAILSRV3
- Domino server using SMTP on the Domino server on AS/400 HOME400
- Domino server using SMTP on the AS/400 system on AS/400 MAILSRV2

The internal DNS can be on any AS/400 system on the network. In our scenario, the AS/400 HOME400 handles this function.

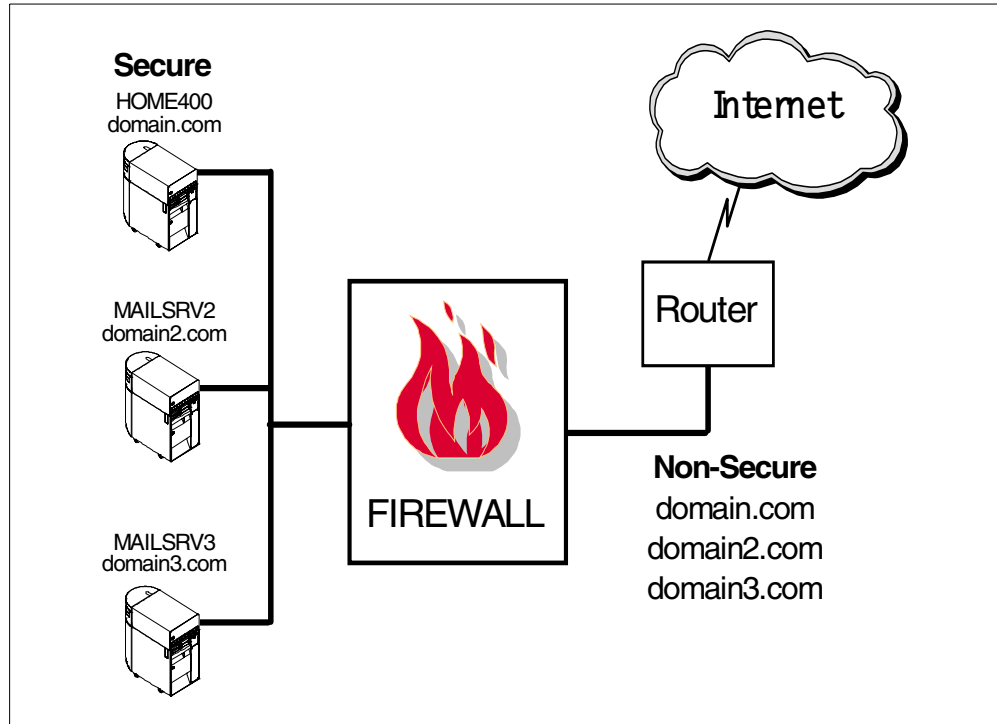


Figure 3. Network configuration for multiple domains on a single server

2.3.4 Single domain with fanout to multiple systems

Chapter 6, “Single domain with a fanout to multiple systems” on page 193, presents the procedures for firewall configurations that support a one-mail-domain environment with multiple mail servers. Figure 4 on page 15 illustrates a logical view of the network configuration used in this scenario. All mail arrives at HOME400 and is then passed to the correct mail server.

In this scenario, we present a company that has one mail domain with multiple AS/400 systems each running a Domino server. The three mail servers are Domino servers using the SMTP support in Domino (not MSF).

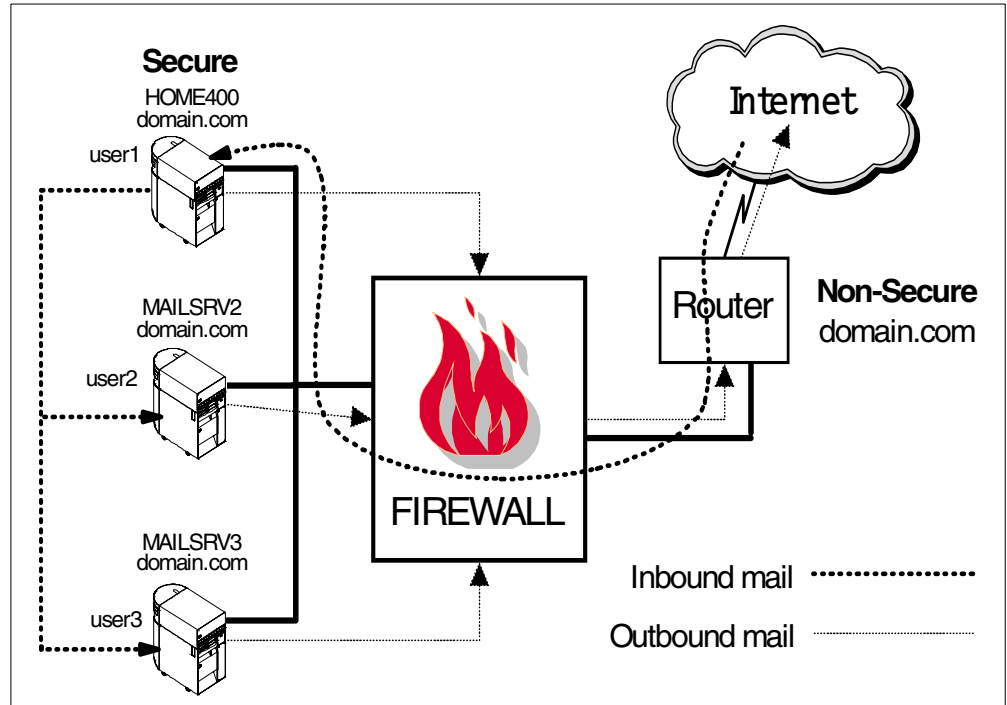


Figure 4. Network configuration for one domain with fanout

Chapter 3. One domain with subdomains on a single system

This chapter presents the procedures for configuring firewalls that support a mail environment composed of one domain with multiple subdomains. All subdomains are processed by the same AS/400 system. The chapter contains procedures for setting up the configuration of both IBM Firewall for AS/400 and IBM eNetwork Firewall for Windows NT. This chapter also contains the procedures that we use to set up an SMTP and POP3 server or SMTP and Domino server on the AS/400 system.

3.1 Scenario

In this scenario, we present a company that has three divisions. Each of these divisions has its own mail domain. The public mail domains and the private mail domains are the same.

The internal DNS can be on any AS/400 system on the network. In our scenario, the AS/400 system named HOME400 provides this function.

If you use the POP3 server, the SMTP server is on the AS/400 HOME400. If you use a Domino server, the SMTP is managed by the Domino server DOM400.

The firewall is either IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT. The firewall filters are open to allow POP3 clients and Domino clients on the Internet to access the internal mail server. Network Address Translation (NAT) is used to map the secure address of the mail server to a public address.

3.1.1 Scenario network configuration

Figure 5 on page 18 illustrates a logical view of the network configuration used in this scenario. There are three ways to implement the firewall:

- The firewall is an Integrated Netfinity Server running IBM Firewall for AS/400.
- The firewall is a separate PC running Windows NT Server and IBM eNetwork Firewall for Windows NT.
- The firewall is an Integrated Netfinity Server running IBM eNetwork Firewall for Windows NT.

The procedure for setting up a Windows NT Server on an Integrated Netfinity Server is provided in Chapter 8, "Installing a Windows NT Server to support firewalls" on page 289.

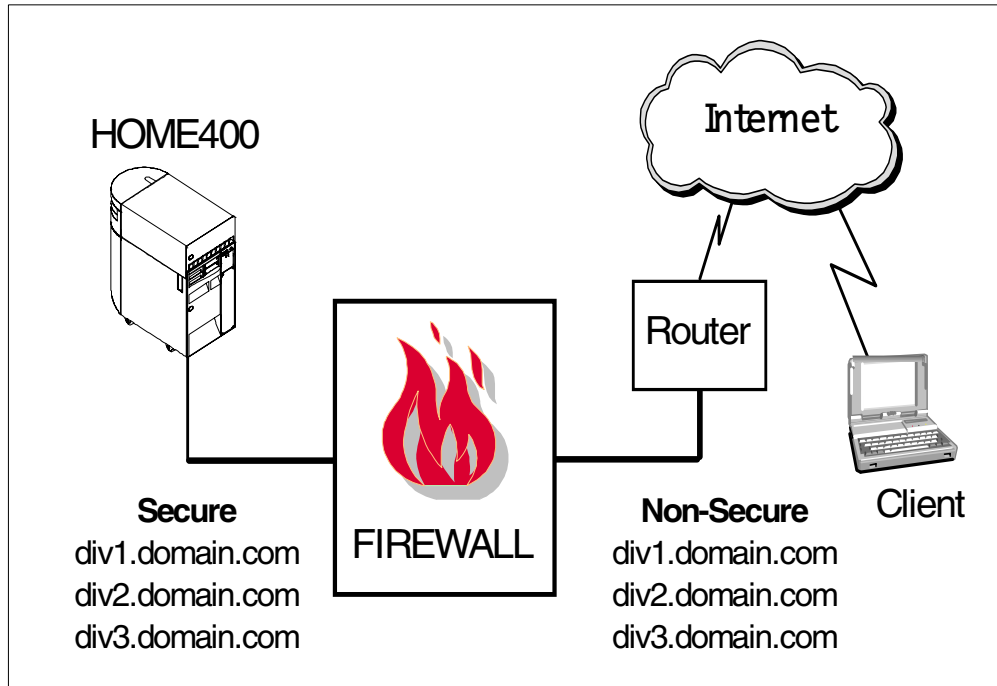


Figure 5. Configuring one domain with subdomains on a single mail server

3.1.2 Scenario objectives

The objectives of this scenario are:

- Configure the IP domains on the internal DNS.
- Configure the firewall so that it can handle the mail domains.
- Open the firewall to let POP3 clients access their mail from the Internet.
- Configure the POP3 server to handle internal and Internet mail.
- Configure the Domino server to handle internal and Internet mail.

3.1.3 Scenario advantages

This scenario has the following advantages:

- The domain *domain.com* is handled by the internal DNS. It is not defined on the firewall and so is not visible from the Internet.
- The firewall can be either IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT.
- IBM Firewall for AS/400 can handle the DNS function, so you do not need to spend extra money to handle this function by your ISP or on other DNS in the DMZ.
- Inbound mail is processed on a single system. This is an opportunity to have an antivirus system scanning mail coming from the Internet.

3.1.4 Scenario limitations

There are also some limitations associated with this scenario. They include:

- The domain *domain.com* is handled by the internal DNS. If you want to add a Web server, *www.domain.com*, to be visible from the Internet, the firewall configuration has to be modified.

- The POP3 client on the Internet needs to access the server *behind* the firewall. This requires that you add filter rules to permit the POP3 traffic through the firewall. This is an issue with any client on the Internet accessing a server which is *behind* the Firewall.
- The DNS function of IBM eNetwork Firewall for Windows NT uses the NT DNS in a cache-only mode. This means that a DNS is needed in the DMZ or you will have to use the DNS of your ISP (using the ISP DNS may mean extra fees).

3.1.5 Planning considerations

Consider the following points when planning for implementation:

- Is there any internal DNS in your company?
- Are the PCs configured to use an internal DNS?
- Are you using AS/400 SMTP and POP or AS/400 Domino for mail?
- Are you using IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT as your firewall?

The remainder of this chapter documents the procedures used to set up the firewall and mail server using both firewall products and both mail products. You should choose the sections that are appropriate for your environment.

- FW1MAIL refers to IBM Firewall for AS/400 system.
- FW1NT refers to IBM eNetwork Firewall for Windows NT system.
- HOME400 refers to the AS/400 system on the domain *domain.com*.
- DOM400 refers to the Domino server on AS/400 HOME400.

Table 4 lists the domain names, host names, and IP addresses used for this scenario.

Table 4. Domain names, host names, and IP addresses

Domain name	Host name	IP address
domain.com	fw1nt (non-secure)	208.222.150.250
domain.com	fw1nt	10.100.1.2
domain.com	fw1mail (non-secure)	208.222.150.250
domain.com	fw1mail	10.100.1.2
domain.com	fw1mail (internal LAN)	192.168.2.2
domain.com	home400	10.100.1.7
domain.com	home400 (internal LAN)	192.168.2.1
domain.com	dom400	10.100.1.8
(Host table entry)	div1.domain.com	10.100.1.3
(Host table entry)	div2.domain.com	10.100.1.4
(Host table entry)	div3.domain.com	10.100.1.5

Table 5 lists the values used to configure the AS/400 DNS for this scenario using different SMTP servers.

Table 5. Secure mail server name - DNS MX values

Firewall product	Secure domain name	MX value for mail server name for AS/400 SMTP	MX value for mail server name for Domino SMTP
IBM Firewall for AS/400	div1.domain.com	home400.domain.com.	dom400.domain.com.
	div2.domain.com	home400.domain.com.	dom400.domain.com.
	div3.domain.com	home400.domain.com.	dom400.domain.com.
IBM eNetwork Firewall for Windows NT	div1.domain.com	home400.domain.com.	dom400.domain.com.
	div2.domain.com	home400.domain.com.	dom400.domain.com.
	div3.domain.com	home400.domain.com.	dom400.domain.com.

Table 6 lists the values used to configure SMTP mail relay on the firewall for this scenario using the different firewall and mail products.

Table 6. Domain name and secure mail server name - Firewall values

Firewall product	Secure and public domain name	Firewall mail server name for AS/400 SMTP	Firewall mail server name for Domino SMTP
IBM Firewall for AS/400	div1.domain.com	div1.domain.com	div1.domain.com
	div2.domain.com	div2.domain.com	div2.domain.com
	div3.domain.com	div3.domain.com	div3.domain.com
IBM eNetwork Firewall for Windows NT	div1.domain.com	home400.domain.com	dom400.domain.com
	div2.domain.com	home400.domain.com	dom400.domain.com
	div3.domain.com	home400.domain.com	dom400.domain.com

In Table 7, list the domain names, host names, and IP addresses that you need for this scenario.

Table 7. User values for domain name, host name, and IP address

Domain name	Host name	IP address

Domain name	Host name	IP address
(Host table entry)		
(Host table entry)		
(Host table entry)		

In Table 8, list the values you need to configure the AS/400 DNS for this scenario.

Table 8. User values for secure mail server name - DNS MX values

Firewall product	Secure domain name	MX value for mail server name for AS/400 SMTP	MX value for mail server name for Domino SMTP

In Table 9, list the values you need to configure the SMTP mail relay on the firewall for this scenario.

Table 9. User values for domain name and secure mail server name - Firewall

Firewall product	Secure and public domain name	Firewall mail server name for AS/400 SMTP	Firewall mail server name for Domino SMTP

3.1.6 Task summary

To set up this scenario, you must configure the DNS to support the mail environment (step 1), configure a firewall (step 2 or 3), and configure your mail server (steps 4 and 5, or step 6).

1. Configure the AS/400 DNS.
2. Configure IBM Firewall for AS/400 (FW1MAIL).
3. Configure IBM eNetwork Firewall for Windows NT (FW1NT).
4. Configure the SMTP server on the AS/400 system.
5. Configure the POP3 mail on the AS/400 system.
6. Configure the Domino server for mail.

3.2 Configuring the AS/400 DNS

This section describes the tasks that you must perform to configure the internal AS/400 DNS to handle one domain with subdomains on a single mail server. If the DNS is not already installed, refer to the redbook *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147.

3.2.1 Task summary

To configure the AS/400 DNS for this scenario, perform the following steps:

1. Configure the AS/400 DNS to handle the internal domain *domain.com*.
2. Add systems to *domain.com*.
3. Add the three subdomains *div1.domain.com*, *div2.domain.com*, and *div3.domain.com*.
4. Configure the MX record for each of the subdomains.
5. Configure the internal DNS to forward the queries to the firewall.

3.2.2 Configuring the AS/400 DNS to handle the internal domain

To configure the AS/400 DNS, you use Operations Navigator, which is included as part of Client Access Express for Windows.

To access the DNS configuration, select your **AS/400 system name** ->**Network**->**Server**->**TCP/IP**. Double-click **DNS**. Click the + symbol beside DNS Server - Home400 (system name in our example). The window shown in Figure 6 is displayed.

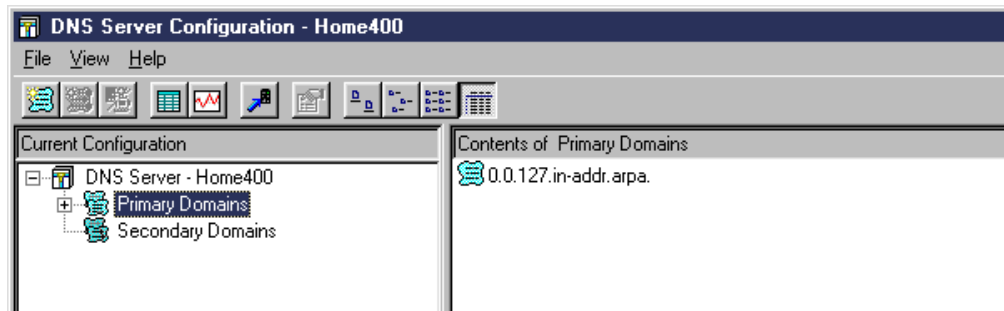


Figure 6. Configuring the AS/400 DNS to handle the internal domain: *domain.com*

To add the primary domain, perform the following procedure:

1. Right-click on **Primary Domains**, and select **New Primary Domain**. The window shown in Figure 7 on page 23 is displayed.

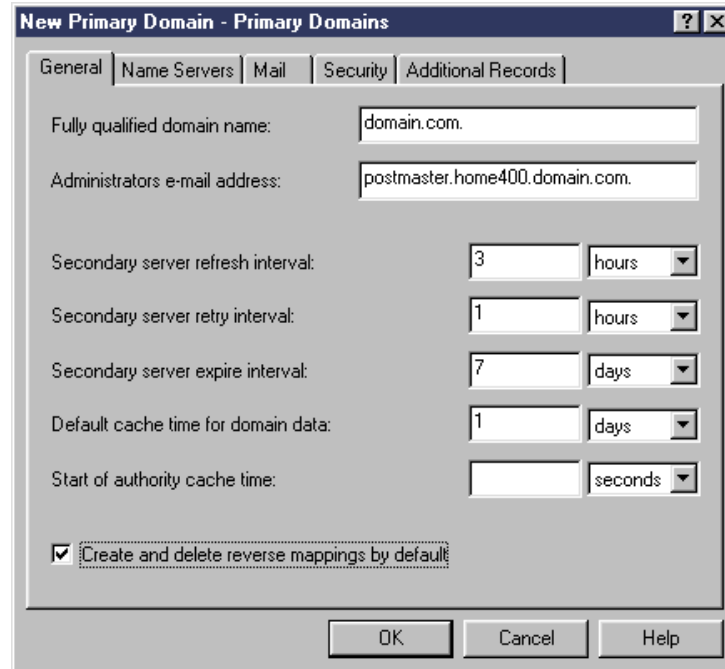


Figure 7. New Primary Domain: domain.com

2. Enter the domain name `domain.com.` You *must* put a dot at the end of your domain since it is a fully qualified domain name.
3. Check **Create and delete reverse mappings by default**.
4. Click **OK**. The window shown in Figure 8 is displayed. Your domain name is displayed in the right-hand frame.
5. Right-click on the domain name you added. A drop-down menu appears. Click **Enable**. This enables the domain in the DNS.

You have now created the domain `domain.com`.

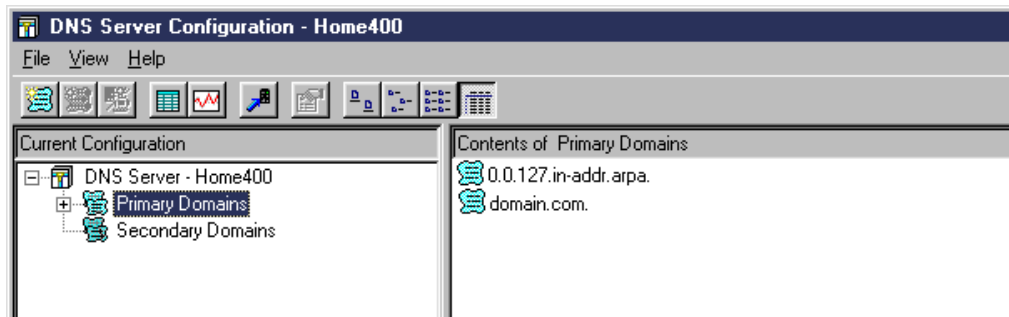


Figure 8. Content of Primary Domains after creating domain.com

3.2.3 Adding systems to the domain

After you create the domain, you need to add the mail server system, the Domino server (if you are using one), and the firewall name. To add the systems, perform the following steps:

1. Right-click **domain.com**.
2. Select **New Host**.
3. Click **Add**. The New Host window is displayed (Figure 9).

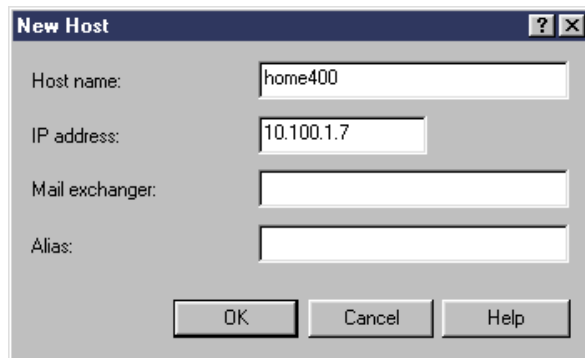


Figure 9. Adding the AS/400 host name

4. Enter the AS/400 host name and the IP address.
5. Click **OK**.

Repeat these steps to add each host name of *domain.com* listed in Table 4 on page 19. Only host names that have a 10.100.1.x IP address need to be stored in the DNS.

Now that you have added the system names to the DNS, continue setting up the DNS.

3.2.4 Adding the subdomains to the DNS

You now must add the three subdomains for which you receive mail to the DNS. In this scenario, the subdomain names are:

- div1.domain.com
- div2.domain.com
- div3.domain.com

The mail domains are the same in the secure and non-secure network. To add the subdomains to the DNS, repeat the steps described in 3.2.2, “Configuring the AS/400 DNS to handle the internal domain” on page 22, for each subdomain.

When you are finished adding all the domains, your DNS Server Configuration window should look similar to the example shown in Figure 10 on page 25. As a result of configuring our scenario, we have the following domains:

- 0.0.127.in-addr-arpa Reverse lookup for loopback domain 127.0.0
- 1.100.10.in-addr-arpa Reverse lookup for 10.100.1 domain
- div1.domain.com Mail domain for division 1
- div2.domain.com Mail domain for division 2
- div3.domain.com Mail domain for division 3
- domain.com Primary domain for systems

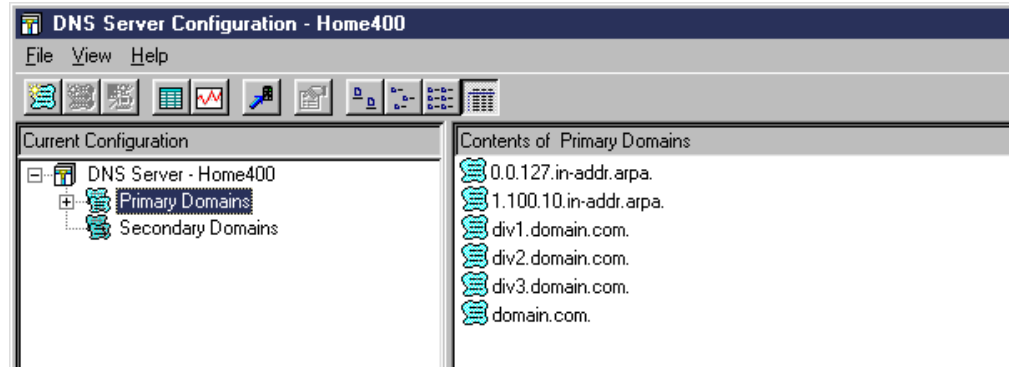


Figure 10. Content of Primary Domains after creating the three subdomains

If any of the domain names have a yellow exclamation mark (!) on them, they need to be enabled. Right-click on the domain name. A drop-down menu appears. Click **Enable**. This enables the domain in the DNS.

Now you need to add the mail exchange (MX) information for each of the mail domains.

3.2.5 Configuring the MX record for each subdomain

The MX record tells the DNS client (it can be either a PC or another DNS) the name of the SMTP server that processes mail for the domain. Complete these steps:

1. Right-click on **div1.domain.com**.
2. Select **Properties**.
3. Click the **Mail** tab.
4. Click **Add**. The window shown in Figure 11 is displayed.

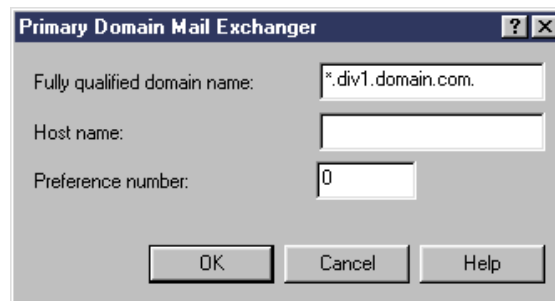


Figure 11. Adding an MX record for a subdomain

5. Remove the asterisk (*) from the front of the default domain name. In this example, we change (*.div1.domain.com.) to div1.domain.com.
6. Enter the fully qualified host name of the SMTP server: home400.domain.com. or dom400.domain.com. Refer to Table 5 on page 20 for the MX record value that refers to the domain. Be sure to include the dot (.) at the end of the host name.
7. Click on **OK**.
8. Click on **OK** a second time to exit the Properties window.

Repeat the steps in this section to create an MX record for domains *div2.domain.com* and *div3.domain.com*.

3.2.6 Configuring the internal DNS to forward the queries to the firewall

The internal DNS cannot answer the queries that are intended for the Internet. It needs to be linked with the DNS firewall.

If e-mail is sent to somebody@us.ibm.com, it first goes to the internal SMTP server. Then, it is forwarded to the firewall. From the firewall, it is sent to the Internet.

To set up DNS forwarding, you must change the DNS properties. You should start at the DNS Server Configuration window shown in Figure 12.

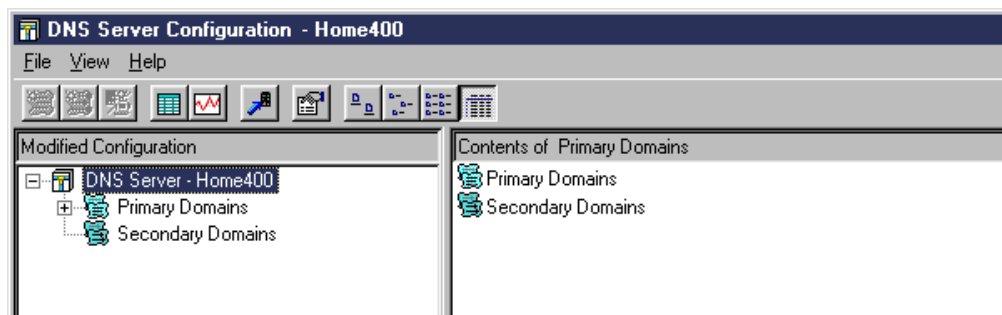


Figure 12. Configuring the internal DNS to forward queries to the firewall

Use the following procedure to change the properties of the DNS:

1. Right-click **DNS Server - Home400**.
2. Select **Properties**.
3. Click the **Forwarders** tab. The window shown in Figure 13 on page 27 is displayed.

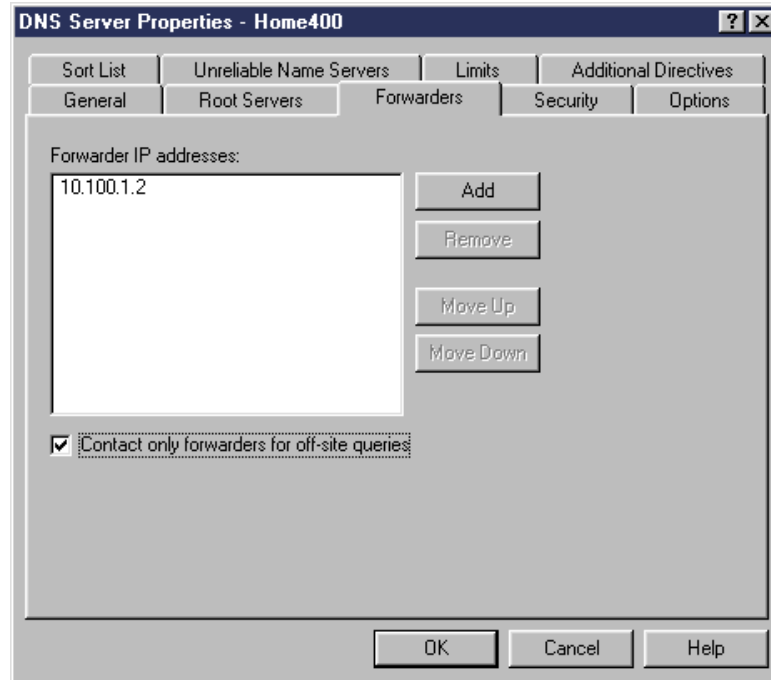


Figure 13. Adding the IP address of the firewall to the forwarders list

4. Click the **Add** button.
5. Enter the secure IP address of the firewall.
6. Check **Contact only forwarders for off-site queries**.
7. Click **OK**.

The DNS configuration is now ready to handle your SMTP mail. Stop and start the DNS server, or click **File->Update Server** to update the DNS server configuration and make your configuration available.

3.3 Configuring IBM Firewall for AS/400 (FW1MAIL)

This section describes the tasks that you must perform to configure IBM Firewall for AS/400 to handle one domain with subdomains on a single mail server.

3.3.1 Scenario network configuration

Figure 14 on page 28 shows the network configuration used in this scenario. In this portion of the scenario, we use an Integrated Netfinity Server to run IBM Firewall for AS/400. The network diagram would be the same if we used IBM eNetwork Firewall for Windows NT on the Integrated Netfinity Server. The *Internal LAN and one LAN adapter make up the secure side of the Network. The other LAN adapter is used to connect to the ISP router.

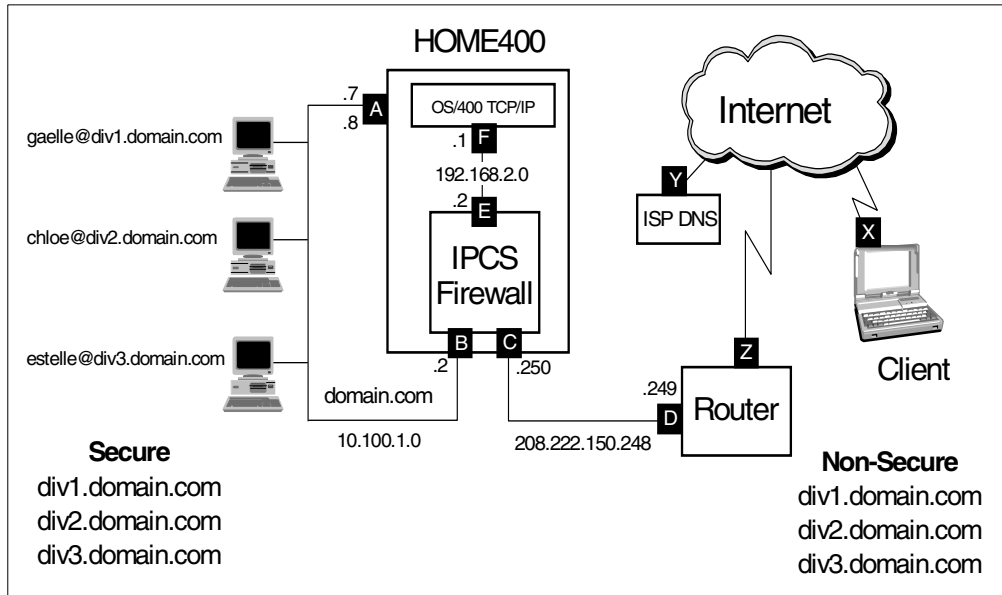


Figure 14. One domain with subdomains on IBM Firewall for AS/400

3.3.2 Task summary

The following list summarizes the tasks used to configure IBM Firewall for AS/400 in this scenario:

1. Install IBM Firewall for AS/400.
2. Perform the basic configuration.
3. Plan NAT to map the POP3 server address outside the firewall.
4. Configure NAT.
5. Start NAT, and turn on IP forwarding.
6. Add the filter rules.
7. Add the filter rules to support Domino access from the Internet.
8. Restart the filters.

3.3.3 Installing IBM Firewall for AS/400 (FW1MAIL)

Install the firewall at the local site using the instructions in the manual *Getting Started with IBM Firewall for AS/400, SC41-5424*. A summary of the installation parameters is shown on the Complete the Firewall Installation summary page in Figure 15 on page 29.



Complete the Firewall Installation

Review the information that you have entered. Make any changes on this page. When you are sure that the information is correct, click the **Install** button to complete the firewall installation. This step takes several minutes to run. Please be patient.

Firewall Name	FW1MAIL													
Firewall Resource Name	CC02													
Router IP Address	208	222	150	249										
Route Destination					Subnet Mask					Next Hop				
	Port 1						Port 2							
LAN Type	Token Ring (16Mb)						Token Ring (16Mb)							
Adapter Address	400000000037						4000000000250							
IP Address	10	100	1	2	208	222	150	250						
Subnet Mask	255	255	255	0	255	255	255	248						

Figure 15. Firewall installation summary page (FW1MAIL)

Start the firewall by clicking **Start** (Figure 16).



Start the Firewall

The firewall takes several minutes to start. Please be patient. Click **Start** to start the firewall.



Figure 16. Starting the firewall (FW1MAIL)

3.3.4 Performing basic configuration (FW1MAIL)

Perform the basic configuration of the local firewall. For further information, refer to *Getting Started with IBM Firewall for AS/400, SC41-5424, and AS/400 Internet Security: IBM Firewall for AS/400, SG24-2162*.

In the Review Configuration, be aware that the *Secure Mail Server* and the *Secure Domain* refer to the internal mail domain name. The SMTP domain name in the inbound e-mail (the value to the right of the @ symbol) is changed to the value in the Secure Mail Server column. This value must match the SMTP mail

address setup for the user on the secure mail server. In our scenario, these values have to be exactly the same because of the domain names we select for our internal users. The value in the Secure Mail Server parameter is used in an MX record DNS query to find the SMTP server that processes the mail. If the query fails, an A record DNS query is done for the value. If an IP address is returned, the mail is routed to the mail server. In most cases, it is easiest to use the same value for the Secure Mail Server and the Secure Domain parameters and let the internal DNS MX records point to the secure mail server system. Refer to Table 6 on page 20 for information about the domain name and secure mail server name.

If you do not have a DNS server in the secure network, this technique will not work and you must specify the fully qualified name of the secure mail server (for example, `hostname.domain.com`) in the Secure Mail Server column. This means that the e-mail address of the users will be in the form `userid@hostname.domain.com`.

In this configuration, we create the three mail domains needed during the basic configuration. This is an easy way to create a domain in IBM Firewall for AS/400. This means that, in this scenario, *domain.com* is *not* visible on the Internet.

We recommend that you link the firewall DNS with multiple DNS in the outside world. If one DNS server fails, you can still continue to send e-mail and surf the Web. In our scenario, the three DNS belong to the ISP.

For more information about IBM Firewall for AS/400, refer to Appendix D, "Firewall concepts" on page 349.

Figure 17 on page 31 and Figure 18 on page 32 show the Review Configuration for FW1MAIL. Refer to Figure 14 on page 28 for the scenario network configuration.



Review Configuration

Review the information that you have entered. Make any changes on this page. When you are sure that the information is correct, print the page for future reference. This creates all the firewall configuration settings. This may take a few minutes to run, so please be patient.

Your AS/400 is: HOME400.DOMAIN.COM

Your firewall is: FW1MAIL

Secure domain name servers:

10.100.1.7

Secure Port	IP Address	Subnet Mask
<input checked="" type="radio"/> Port 1	10.100.1.2	255.255.255.0
<input type="radio"/> Port 2	208.222.150.250	255.255.255.248

Secure Mail Server	Secure Domain	Public Domain
div1.domain.com	div1.domain.com	div1.domain.com
div2.domain.com	div2.domain.com	div2.domain.com
div3.domain.com	div3.domain.com	div3.domain.com

Name Server	IP Address
dns1.isp.com	194.41.0.4
dns2.isp.com	128.9.0.107
dns3.isp.com	192.33.4.12

Figure 17. Basic firewall configuration summary page for FW1MAIL (Part 1 of 2)

Note

When you use subdomains, you must list all the subdomains before the parent domain. In the example shown in Figure 17, we did not add the parent domain domain.com. If we needed to accept mail for the parent domain and the subdomains, we would have added domain.com after the div3.domain.com entry. If the parent domain is listed first, the subdomains will never be found.

Public Server	Public IP Address	Private IP Address

Services	Proxy	SOCKS	NAT
HTTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HTTPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FTP (passive)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FTP (active)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Telnet	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Secure Telnet		<input type="checkbox"/>	<input type="checkbox"/>
Gopher	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WAIS			<input type="checkbox"/>
IRC		<input type="checkbox"/>	<input type="checkbox"/>
RealAudio			<input type="checkbox"/>
Lotus Notes		<input type="checkbox"/>	<input type="checkbox"/>
LDAP		<input type="checkbox"/>	<input type="checkbox"/>
Secure LDAP		<input type="checkbox"/>	<input type="checkbox"/>
Server Mapper		<input type="checkbox"/>	<input type="checkbox"/>
DRDA		<input type="checkbox"/>	<input type="checkbox"/>
POP3 Mail		<input type="checkbox"/>	<input type="checkbox"/>
NNTP		<input type="checkbox"/>	<input type="checkbox"/>
Secure NNTP		<input type="checkbox"/>	<input type="checkbox"/>

If you selected any NAT services, then specify the translation of private to public IP addresses.

NAT	IP Address	Mask
Private	10.100.1.2	255.255.255.0
Public		

OK Cancel

Figure 18. Basic firewall configuration summary page for FW1MAIL (Part 2 of 2)

The firewall is now ready to perform the basic configuration. Complete these steps:

1. Click **OK**. A confirmation page is shown (Figure 19), which indicates that the firewall is configured.



You have successfully configured the firewall. The next step is to restart the firewall servers so that your configuration changes take effect. This will only take a short time. Do you want to restart the firewall?

Figure 19. Confirmation that the firewall is configured

2. Click **Yes**.

3.3.5 Planning NAT to map the POP3 server address outside the firewall

To hide the internal addresses of the POP3 server, we use NAT to map the IP address of the non-secure port of the firewall. However, whenever you permit new traffic through the firewall, you are opening a door in your firewall. Every door that you open creates risks to your secure network.

The *public IP address* for the POP3 server is the same as the non-secure port of the firewall (208.222.150.250). This is possible because port 110 for POP3 is not used on the firewall.

Consider the following points when planning to implement a firewall using the NAT function:

- Determine the server and port to which access is allowed. Notice that you can use the same public address (for example, the non-secure port of the firewall) in multiple MAP settings if you map to different ports.
- The firewall non-secure port IP address and the public IP addresses assigned to servers behind the firewall *must* be on different subnets (except for special cases where the IP address assigned to the public servers is the same as the non-secure port of the firewall).
- Determine the ISP router configuration. Plan to configure the ISP router correctly.
- If the *public IP address* is the same as the firewall's non-secure IP address, no routes are required.
- If the *public IP address* is another address, the router must be configured so that it routes traffic for the *public IP address* using the firewall's non-secure IP address.

Note

In our scenario, we decided to allow the POP3 traffic through the firewall, but it can be any TCP/IP application, such as Domino or Client Access.

In this environment, IBM Firewall for AS/400 can route the traffic destined to the internal POP3 server directly to the AS/400 main processor over the internal LAN (system bus). We assume that the internal LAN address, 192.168.2.1, is the

POP3 server's real IP address. Since we are using NAT, IP forwarding must be permitted.

3.3.6 Configuring NAT

We now start to configure NAT. NAT only provides address translation. Filter rules are added later. Complete this process:

1. Click **NAT** on the Configuration Menu page (Figure 20).

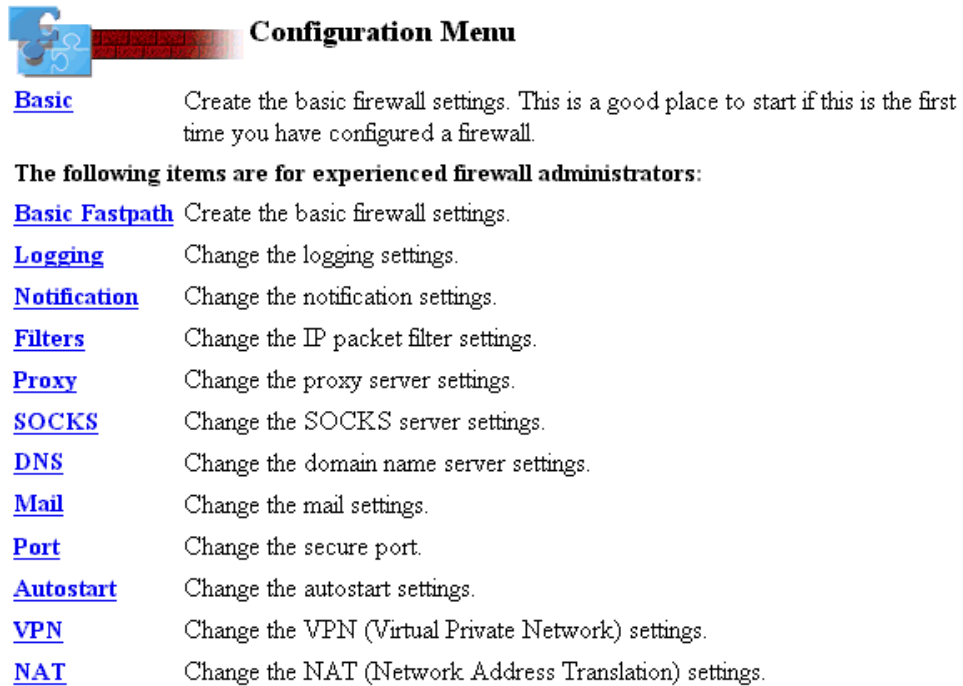


Figure 20. Selection of NAT from the Configuration Menu

The Network Address Translation Settings page is displayed as shown in Figure 21.

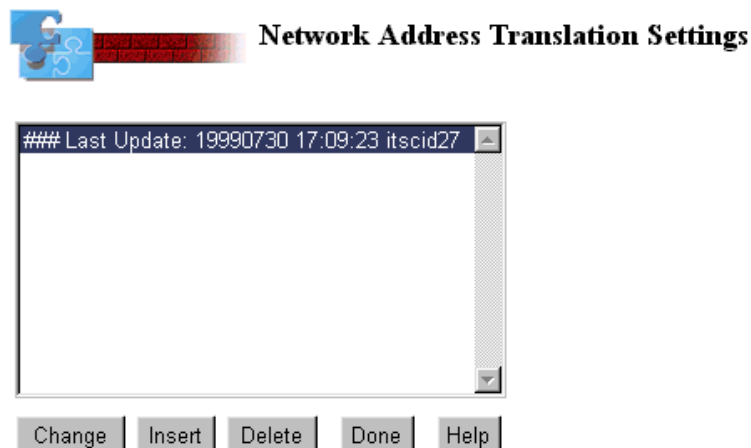


Figure 21. Network Address Translation Settings page

2. Click **Insert**. The window in Figure 22 on page 35 appears.

Insert Network Address Translation



Figure 22. Insert NAT directive

3. Select **MAP**, and click **OK**.

Figure 23 displays the Create Network Address Translation window. Enter the private IP address and private port, followed by the public IP address and public port.

Create Network Address Translation

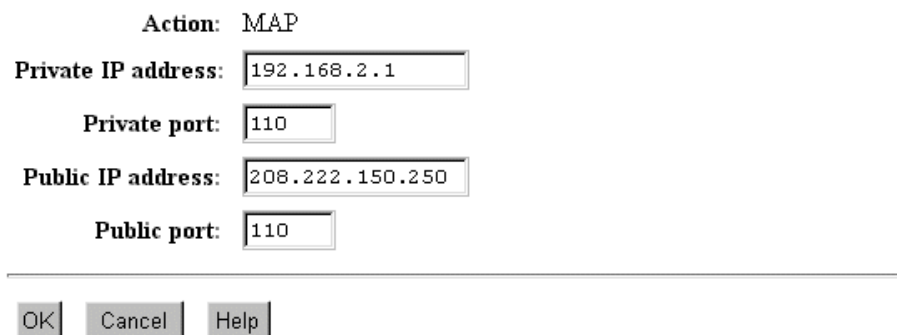
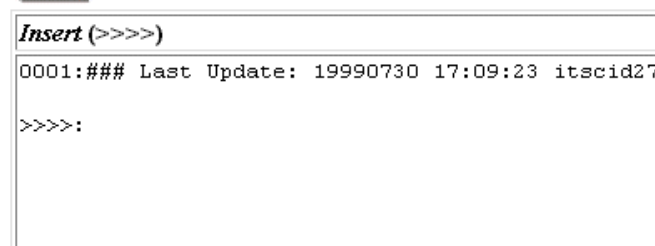


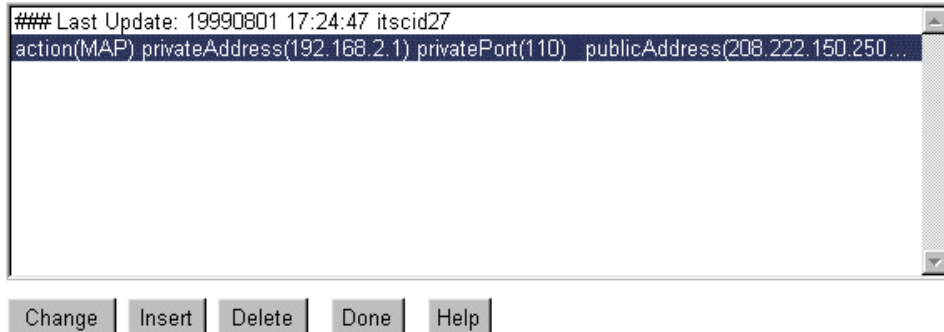
Figure 23. Creating a NAT MAP setting

Enter 110 for the POP3 server for Private port and Public port.

4. Click **OK** to continue.

The resulting NAT setting page is shown for confirmation (Figure 24 on page 36). If you have more settings to add, you can add them now. In this scenario, this is the only NAT setting we need to add. The port used by Domino is 1352.

Network Address Translation Settings



Last Update: 19990801 17:24:47 itscid27
action(MAP) privateAddress(192.168.2.1) privatePort(110) publicAddress(208.222.150.250...

Change Insert Delete Done Help

Figure 24. Displaying NAT Settings

5. Click **Done**.

3.3.7 Starting NAT and turning on IP forwarding

You must now start NAT and permit IP forwarding. Follow these steps:

1. Click the **Administration** icon. Then, click **Status** from the Administration Menu page. Start NAT as shown in Figure 25.

Status

DNS	Started
Proxy	Started
SOCKS	Started
Mail	Started
NAT	Start
Filter	Started
Administration	Started
Logging	Started
IP Packet Forwarding	Permitted

OK Refresh Done Help

Figure 25. Starting NAT and IP forwarding from the Status window

2. Select **Start** for NAT.
3. Select **Permitted** for IP Packet Forwarding.

4. Click **OK**.
5. Click **Done**.

3.3.8 Adding filter rules

Additional filter rules are necessary for any public server behind the firewall, for example, the POP3 server in our scenario. We recommend that you create a section at the bottom of the filter rules just before the *Ending defense* section. Give it a title such as *Custom Rules*. This ensures that you do not override the rules that Basic configuration created. It also makes it easier to recognize rules that you manually add after the initial configuration of the firewall.

Tip

When adding a section for special filtering rules, begin the section with a Description Only rule. Begin the description with a # symbol to make it stand out. Refer to Figure 26 for an example.



The setting has been changed. You must restart the IP packet filter for this change to take effect.

Select an entry and the option to perform:

```
# ### Custom Rules
# #####
#
action(permit) from(any) to(208.222.150.250) protocol(tcp ge 1024/eq 110) interface(no...
action(permit) from(any) to(192.168.2.1) protocol(tcp ge 1024/eq 110) interface(secure...
action(permit) from(192.168.2.1) to(any) protocol(tcp/ack eq 110/ge 1024) interface(se...
action(permit) from(192.168.2.1) to(any) protocol(tcp/ack eq 110/ge 1024) interface(no...
#
#####
### Ending defense
```

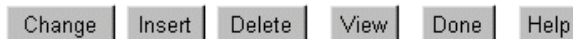


Figure 26. Custom rules inserted prior to the ending defenses

You need to add the following rules to allow POP3 clients on the Internet to access the POP3 server behind the firewall in this scenario:

```
0001:action(permit) from(any) to(208.222.150.250 255.255.255.255) protocol(tcp)
from operation/port(ge 1024) to operation/port(eq 110) interface(non-secure)
routing(both) direction(inbound) fragment(y) log(n) vpn(0) description("
Permit inbound NAT POP3 requests")
0002: action(permit) from(any) to(192.168.2.1 255.255.255.255) protocol(tcp)
from operation/port(ge 1024) to operation/port(eq 110) interface(secure)
routing(route) direction(outbound) fragment(y) log(n) vpn(0)
description("Permit outbound NAT POP3 requests")
0003: action(permit) from(192.168.2.1 255.255.255.255) to(any)
protocol(tcp/ack) from operation/port(eq 110) to operation/port(ge 1024)
```

```

interface(secure) routing(route) direction(inbound) fragment(y) log(n) vpn(0)
description("Permit inbound NAT POP3 replies")
0004: action(permit) from(192.168.2.1 255.255.255.255) to(any)
protocol(tcp/ack) from operation/port(eq 110) to operation/port(ge 1024)
interface(non-secure) routing(route) direction(outbound) fragment(y) log(n)
vpn(0) description("Permit outbound NAT POP3 replies")

```

Note

The numbers 0001 through 0004 are just an example of these rules. We recommend that you place these rules towards the end of the filter rules before the *End defense*. Rule 0004 has a source address of 192.168.2.1 because it has not passed through the NAT process. Refer to *IBM Firewall for AS/400 V4R3: VPN and NAT Support, SG24-5376*, for a discussion on the sequence of events that takes place with regard to NAT and the application of filter rules to a packet.

3.3.9 Restarting filters

To restart the filters, click the firewall **Administration** icon. Then, click **Status** from the Administration Menu page. Select **Restart** for the filters, and click **OK**. Refer to Figure 25 on page 36 for an example of the Status page.

3.3.10 Filter rules to allow Domino access from the Internet

Since we are also using a Domino server on HOME400, you may want to open the firewall to give remote Lotus Notes clients access to it. One way for these clients to have access is through the Internet. By default, Domino does not encrypt the data that it sends. Be aware that this data is sent in the clear over the Internet. You may select encryption in the Notes Client.

To enable a Domino client on the untrusted side of the firewall to have access to the Domino server on the secure side of the firewall, you *must* add filter rules. The Domino server listens on port 1352 for Lotus Notes clients.

Use the procedure in 3.3.8, "Adding filter rules" on page 37, to add the following rules to the firewall filter rules:

```

0001:action(permit) from(any) to(208.222.150.250 255.255.255.255)
protocol(tcp) from operation/port(ge 1024) to operation/port(eq 1352)
interface(non-secure) routing(both) direction(inbound) fragment(y) log(n)
vpn(0) description(" Permit non-secure inbound Domino requests and
replies")
0002: action(permit) from(any) to(192.168.2.1 255.255.255.255) protocol(tcp)
from operation/port(ge 1024) to operation/port(eq 1352) interface(secure)
routing(route) direction(outbound) fragment(y) log(n) vpn(0)
description("Permit secure outbound Domino requests and replies")
0003: action(permit) from(192.168.2.1 255.255.255.255) to(any) protocol(tcp)
from operation/port(eq 1352) to operation/port(ge 1024) interface(secure)
routing(route) direction(inbound) fragment(y) log(n) vpn(0)
description("Permit secure inbound Domino requests and replies")
0004: action(permit) from(192.168.2.1 255.255.255.255) to(any) protocol(tcp)
from operation/port(eq 1352) to operation/port(ge 1024) interface(non-secure)
routing(route) direction(outbound) fragment(y) log(n) vpn(0)
description("Permit non-secure outbound Domino requests and replies")

```

Note

This set of rules specifies a port value of 1352, which is different than the other rule sets for this scenario. Also, the first set of rules specifies `TCP/ACK` in the last two (response) rules, while this set specifies `TCP` only. By having `TCP` in the protocol, the Domino server can start `TCP/IP` sessions, as well as respond to sessions.

IBM Firewall for AS/400 configuration is now ready. For more information about IBM Firewall for AS/400, refer to Appendix D, “Firewall concepts” on page 349.

3.4 Configuring IBM eNetwork Firewall for Windows NT (FW1NT)

This section describes the tasks that you must perform to configure the IBM eNetwork Firewall for Windows NT to handle one domain with subdomains on a single mail server.

3.4.1 Scenario network configuration

The network configuration for this scenario is shown in Figure 27.

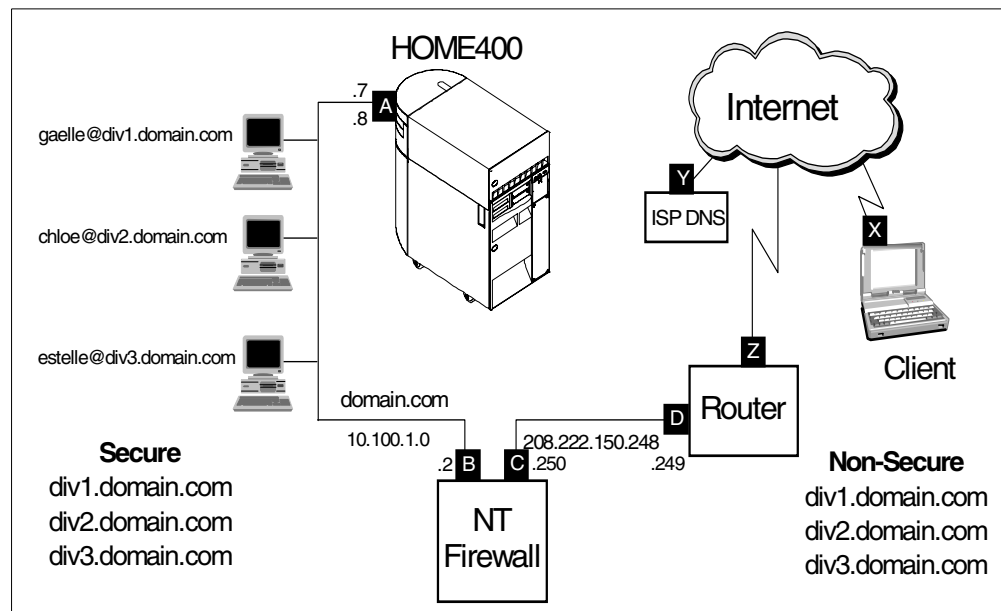


Figure 27. One domain with subdomains on IBM eNetwork Firewall for Windows NT

3.4.2 Task summary

The following list summarizes the tasks used to configure IBM eNetwork Firewall for Windows NT:

1. Install IBM eNetwork Firewall for Windows NT.
2. Set up IBM eNetwork Firewall for Windows NT.
3. Plan NAT to map the POP3 server address outside the firewall.
4. Configure the Windows NT system (FW1NT).
5. Configure NAT.

6. Add new rules.
7. Create a service.
8. Create a network object.
9. Create a connection.
10. Activate the rules.
11. Filter rules to allow Domino access from the Internet.

3.4.3 Installing IBM eNetwork Firewall for Windows NT (FW1NT)

Install the firewall on the Windows NT PC using the instructions in *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT*, SG24-5209. If you do not have this redbook and do not have Internet access to download it, complete the following tasks:

1. Install the Windows NT server operating system.
2. Install the DNS Server for the Windows NT server.
3. Install Service Pack 4 for the Windows NT server. Use Service Pack 5 if available. Service Pack 4 is required. Do not install IBM eNetwork Firewall for Windows NT on the system with the above service pack.
4. Create a local user with Administrator authority.
5. Install the NDIS intermediate driver.
6. Activate IP forwarding in the TCP/IP parameters.
7. Install the firewall product. You must also install the Netscape Web browser so that you can access IBM eNetwork Firewall for Windows NT help text.

3.4.4 Setting up IBM eNetwork Firewall for Windows NT

Complete the following steps to set up IBM eNetwork Firewall for Windows NT:

1. Run the **Configuration Client** in the IBM Firewall folder.
2. Log in with a user that has administrator authority.
3. To start basic configuration, click **Setup Wizard** in the Help menu (Figure 28).

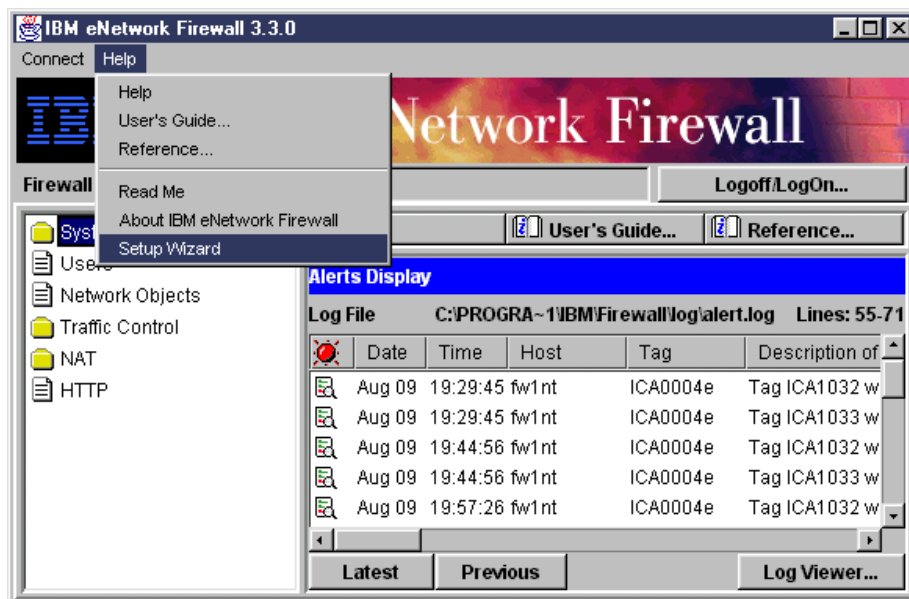


Figure 28. Starting the firewall wizard

4. The Welcome window appears (Figure 29). Read the window carefully.



Figure 29. Firewall wizard welcome screen

5. Click **Next**. The window shown in Figure 30 appears. Read the window carefully.

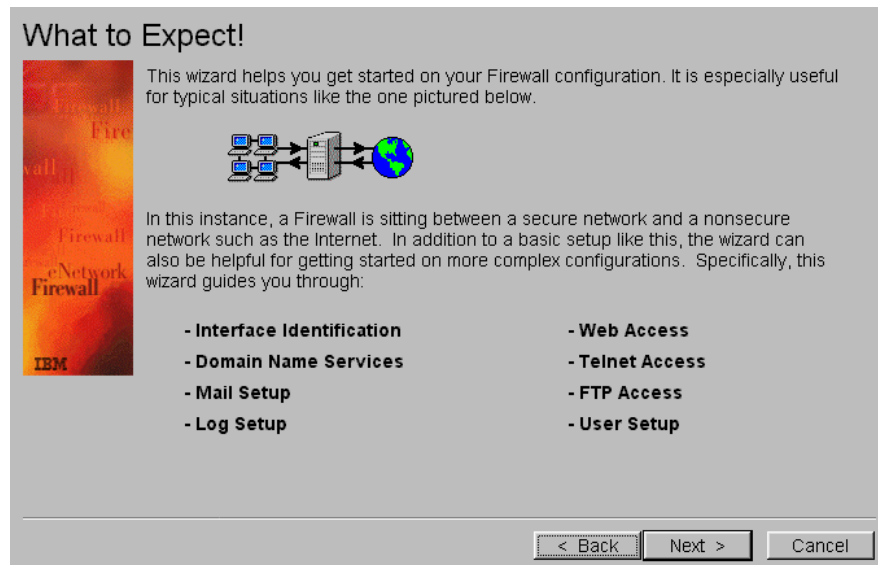


Figure 30. What to Expect firewall wizard

6. Click **Next**. The window shown in Figure 31 on page 42 appears. Read the window carefully.



Figure 31. Important notice firewall wizard

7. Click **Next**. The window shown in Figure 32 appears. Choose the secure interface.

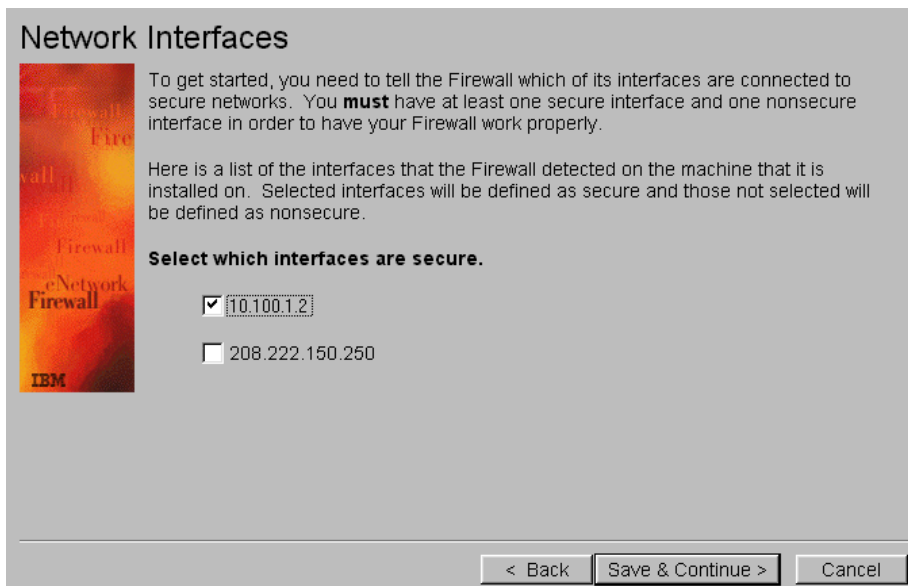


Figure 32. Network interface selection

8. Click **Save & Continue**. The window shown in Figure 33 on page 43 appears.

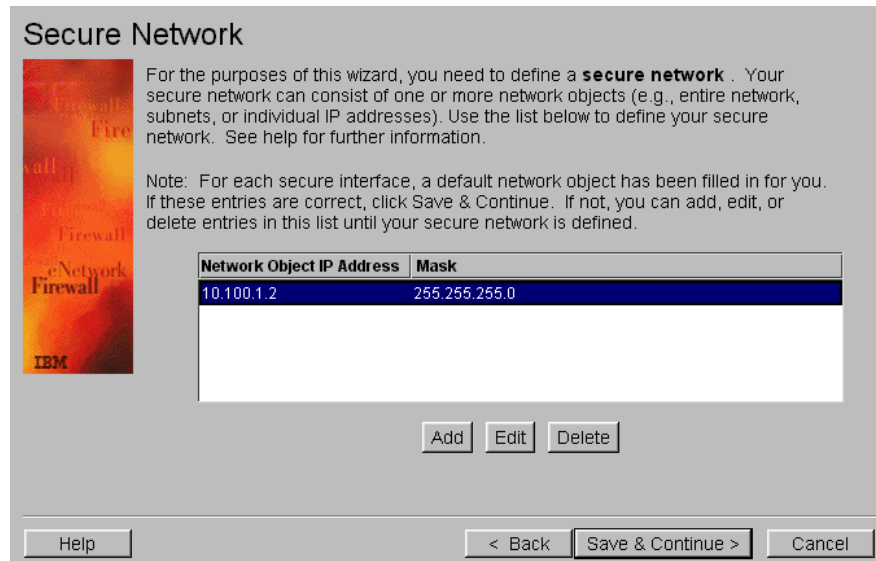


Figure 33. Secure Network configuration

9. Define your secure network. In the window in Figure 33, the wizard guesses that your secure network is any IP address that starts with 10.100.1.
10. Click **Save & Continue**. The window shown in Figure 34 appears.

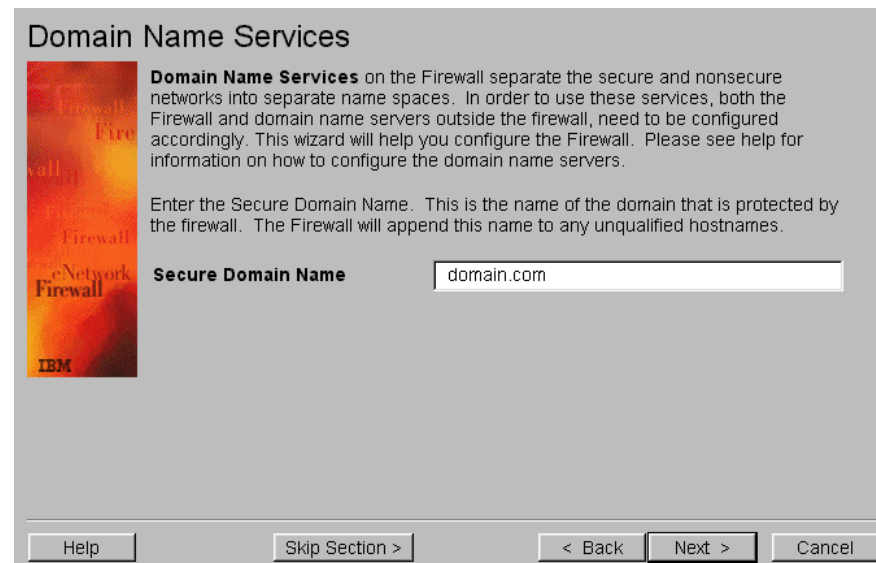


Figure 34. Domain Name Services

11. In the window shown in Figure 34, enter the name of your internal domain name. This domain is protected by your firewall. IBM eNetwork Firewall for Windows NT uses NT DNS in a cache-only mode. The secure domains are already stored in the AS/400 DNS. For non-secure domains, your ISP can handle this function, or you can install an extra DNS in the DMZ.
12. Click **Next**. The window shown in Figure 35 on page 44 appears.

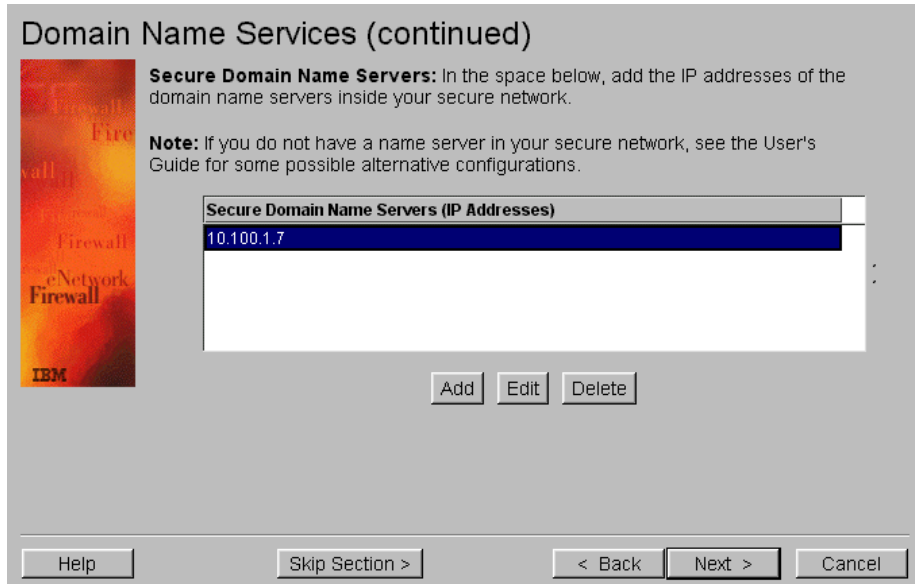


Figure 35. Secure DNS IP address

13. Enter the IP Address of the secure internal DNS.

14. Click **Next**. The window shown in Figure 36 appears.

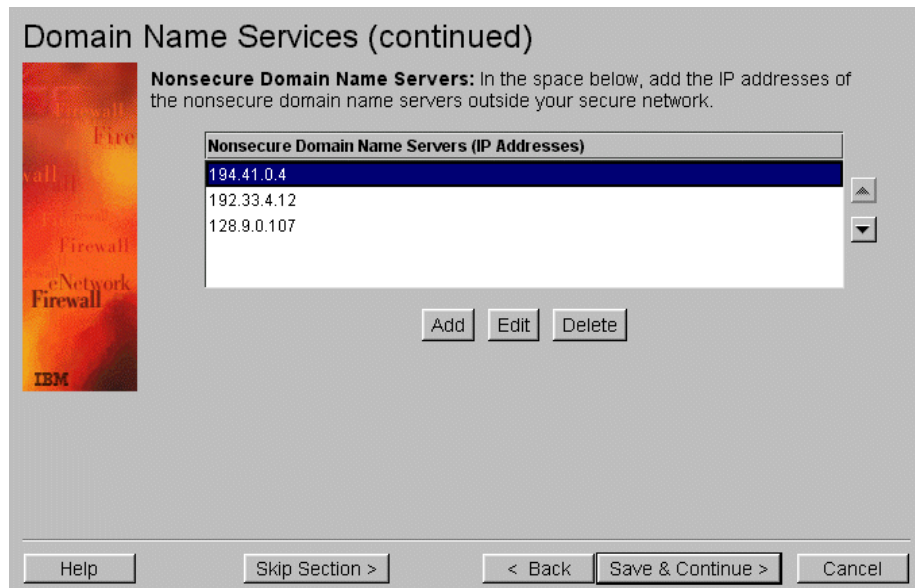


Figure 36. Non-secure DNS IP addresses

15. Click **Add**.

16. Enter the IP address of the non-secure DNS (ISP DNS).

17. Click **Next**.

18. Repeat steps 15 through 17 if the firewall DNS is linked with more DNS (recommended).

19. Click **Save & Continue**. The window shown in Figure 37 on page 45 appears.

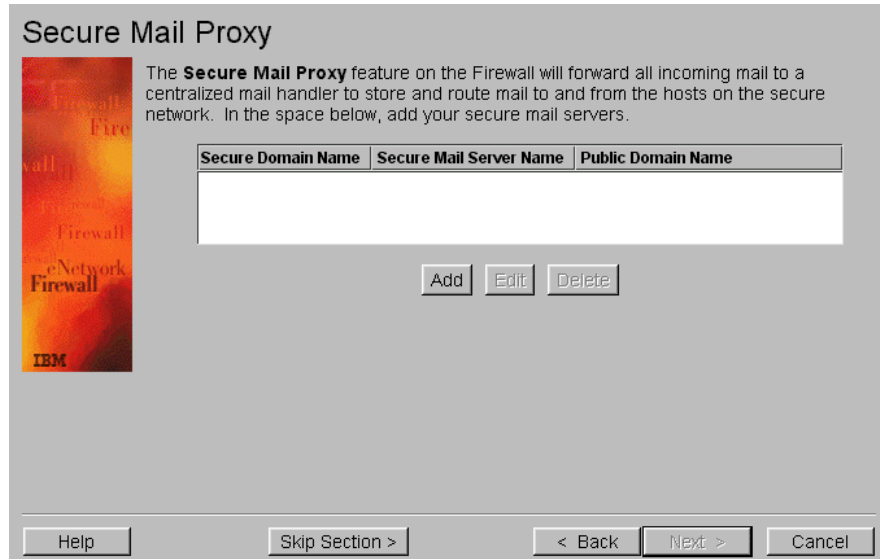


Figure 37. Secure Mail Proxy

20. Click **Add**. The window shown in Figure 38 appears.



Figure 38. Add a secure mail server

21. Enter your Secure Domain Name, Secure Mail Server Name, and Public Domain Name. Refer to Table 6 on page 20 for information about domain names and secure mail server names. Click **Save & Continue**. The window shown in Figure 39 on page 46 appears.

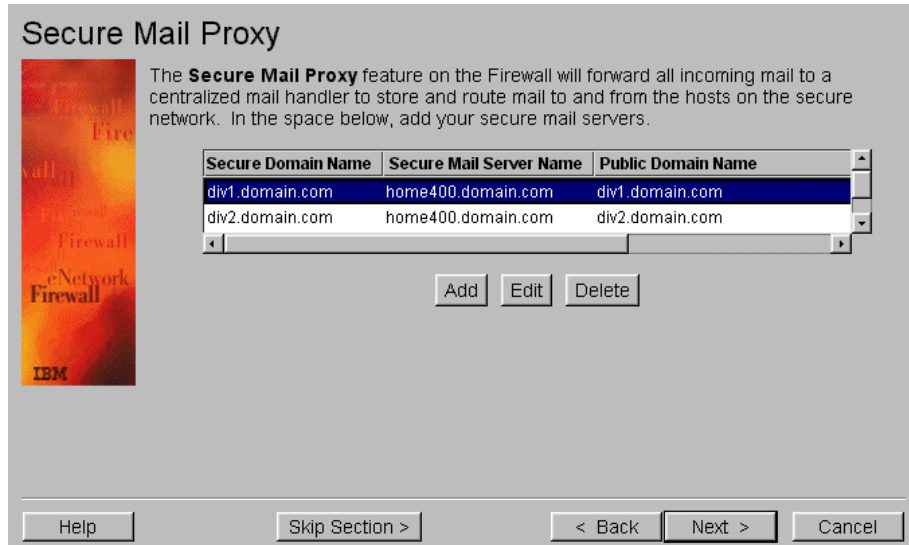


Figure 39. Secure Mail Proxy display

22.Repeat steps 20 and 21 for *div2.domain.com* and *div3.domain.com*.

23.Click **Next**. The window shown in Figure 40 appears.

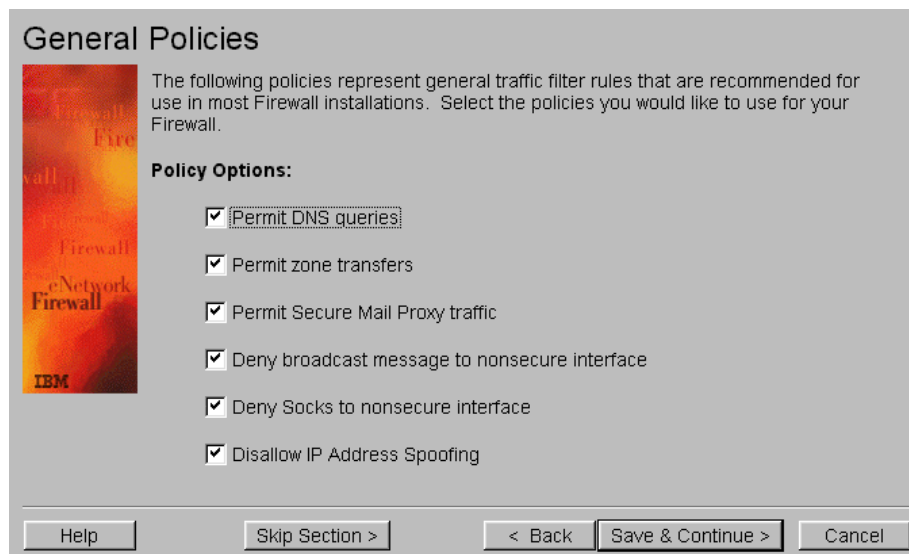


Figure 40. Security policies configuration

24.The marked options that you see under Policy Options are recommended for most firewall installations. Click **Save & Continue**. The window shown in Figure 41 on page 47 appears.

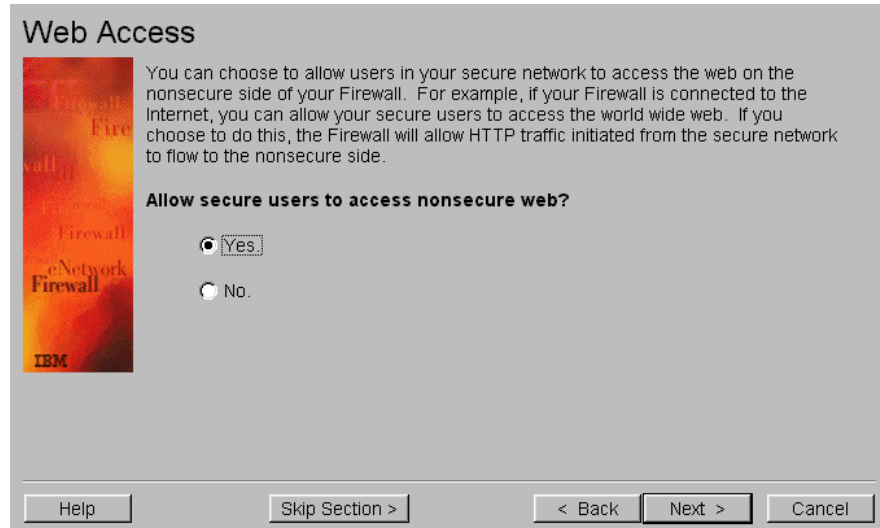


Figure 41. Web Access

25. Select **yes** or **no** for whether to allow Internet access to users. Click **Next**. The window shown in Figure 42 appears.

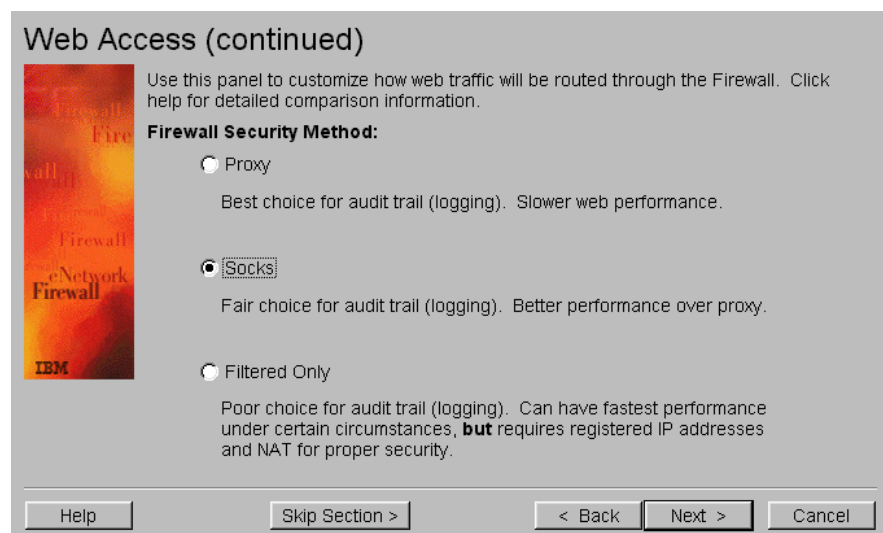


Figure 42. Web Access via Proxy, Socks, or Filtered Only

26. Define which Web access best matches your company. Click **Next**. The window shown in Figure 43 on page 48 appears.

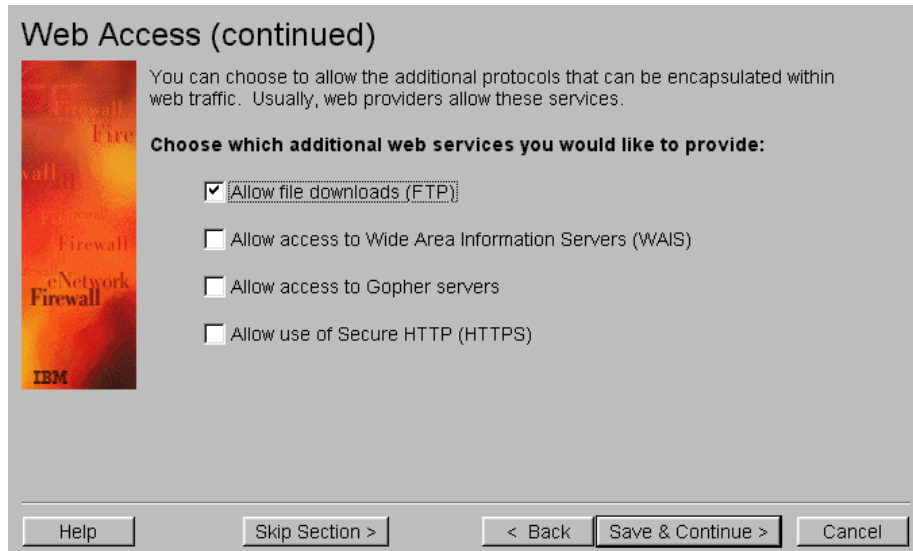


Figure 43. Web Access services

27. Select which services are allowed. Click **Save & Continue**. The window shown in Figure 44 appears.

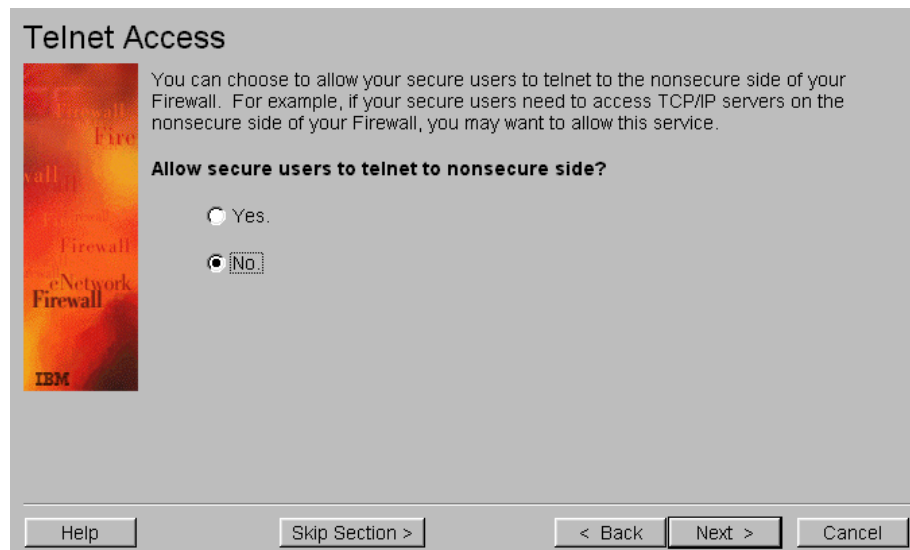


Figure 44. Telnet Access

28. Select **yes** or **no** for whether to allow Telnet access on the non-secure port of the firewall. Click **Next**. The window shown in Figure 45 on page 49 appears.

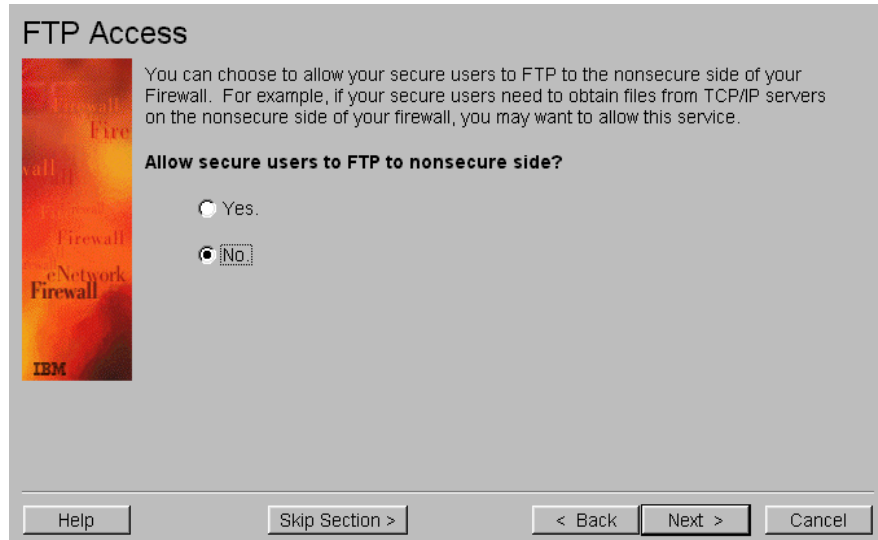


Figure 45. FTP Access

29. Select **yes** or **no** for whether to allow FTP access on the non-secure port of the firewall. Click **Next**. The window shown in Figure 46 appears.

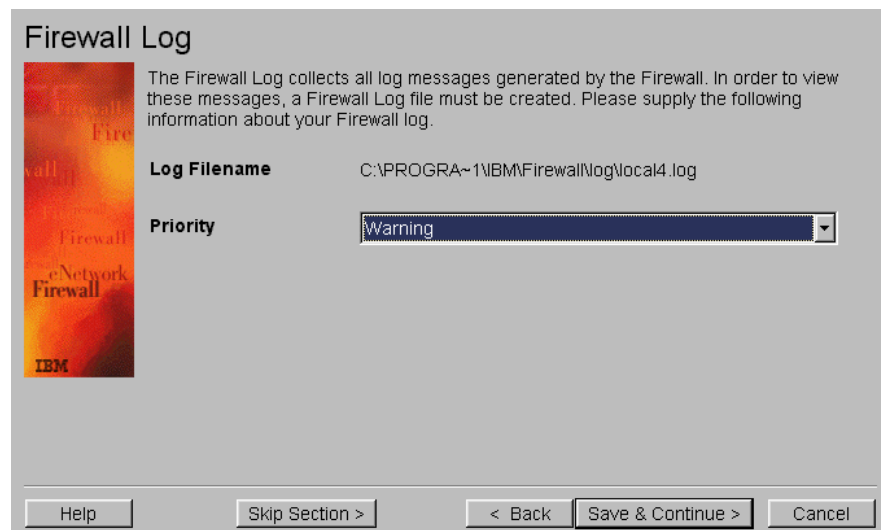


Figure 46. Firewall Log

30. Choose the level of the logs that are stored on the firewall database. Click **Save & Continue**. The window shown in Figure 47 on page 50 appears.

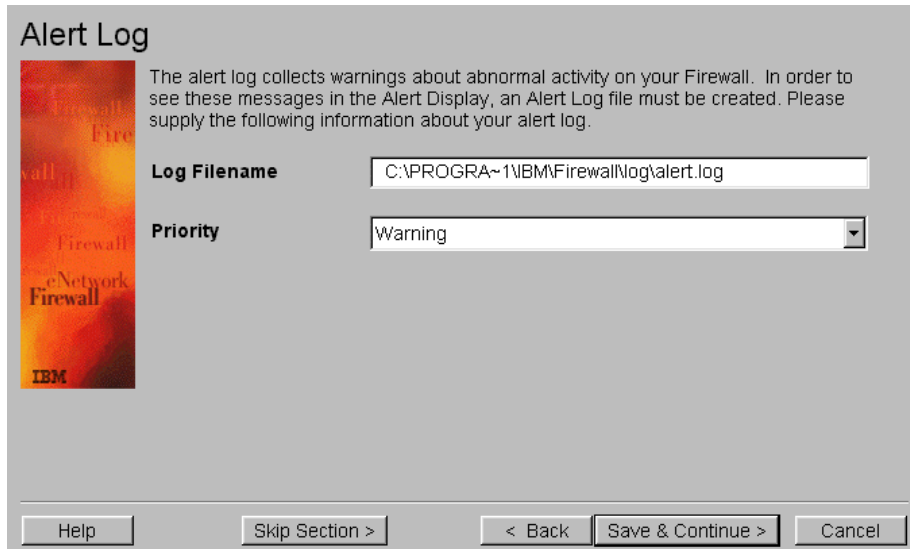


Figure 47. Alert Log

31. Choose the level of the logs that are stored on the alert database. Click **Save & Continue**. The window shown in Figure 48 appears.

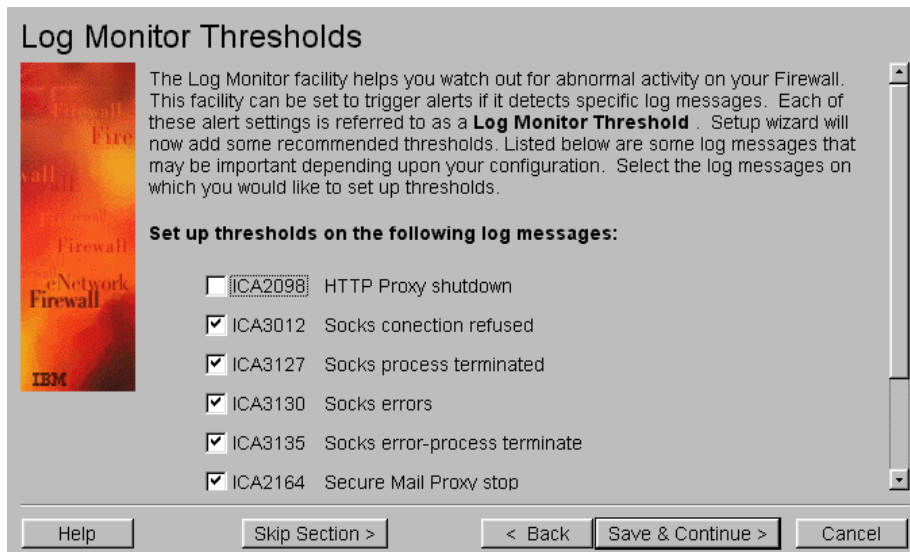


Figure 48. Log Monitor Thresholds

32. Select the thresholds. Click **Save & Continue**. The window shown in Figure 49 on page 51 appears.

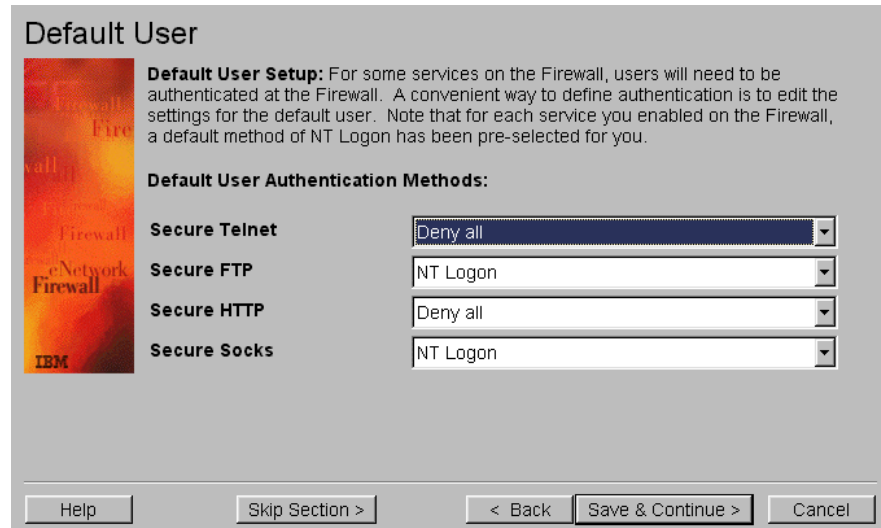


Figure 49. Default User Setup

33. For some services, a firewall user needs to be authenticated. Click **Save & Continue**. The window shown in Figure 50 appears.



Figure 50. Setup activation

34. Choose whether to activate your configuration now or at a later time. Click **Finish**.

3.4.5 Planning NAT to map POP3 server address outside the firewall

To hide the internal addresses of the POP3 server, we use NAT to map the IP address. However, whenever you permit new traffic through the firewall, you are opening a door in your firewall. Every door that you open creates risks to your secure network.

The *registered IP address* for the POP3 server that we use is in the same subnet as the non-secure port of the firewall (208.222.150.250).

Consider the following points when planning to implement a firewall using the NAT function:

- Determine the server and port to which access is allowed. Notice that you can use the same public address with different ports.
- Determine the ISP router configuration. Plan to configure the ISP router correctly, if needed.
- If the registered IP address is on another subnet, the router must be configured so that it routes traffic for the registered IP address.
- If the registered IP address is in the same subnet as the firewall's non-secure IP address, you need to get the firewall host to respond to ARP requests for the NAT IP addresses with the MAC address of the non-secure adapter. On Windows NT, you do this by specifying the NAT IP addresses as a second address of your non-secure adapter.

3.4.6 Configuring the Windows NT system (FW1NT)

The procedure to define a second IP address on Windows NT is explained here:

1. Open the **network** in the Control Panel folder.
2. Choose the **protocol** tab, and open **TCP/IP** properties.
3. Click **Advanced**, and select the non-secure adapter (Figure 51).
4. Enter any additional IP addresses that you may need for NAT. You *must* reboot to activate the second IP address.

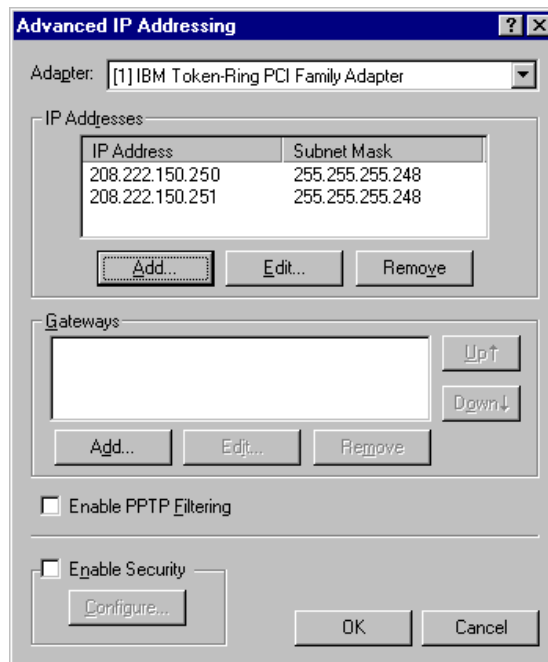


Figure 51. Advanced IP Addressing

3.4.7 Configuring NAT

NAT only provides address translation. Filter rules are added later. Follow these steps to configure NAT:

1. To create a new NAT setting, double-click **SETUP** in the NAT folder in the navigation tree.

The window in Figure 52 is displayed.

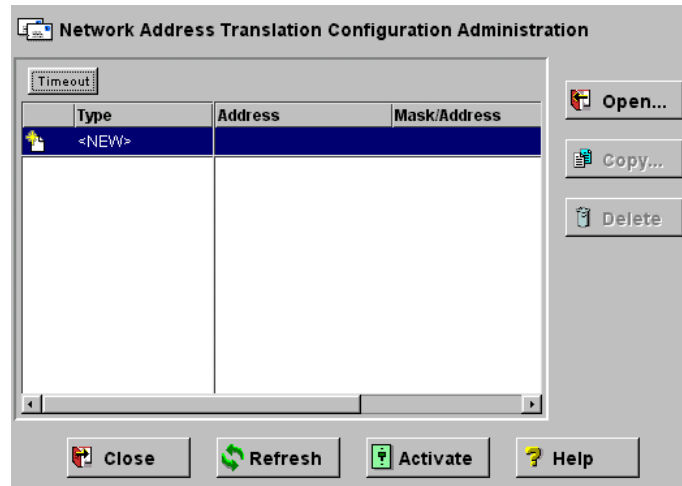


Figure 52. Network Address Translation Configuration Administration

2. Double-click **NEW**. The window shown in Figure 53 appears.
3. Choose **Map** for Type of NAT.

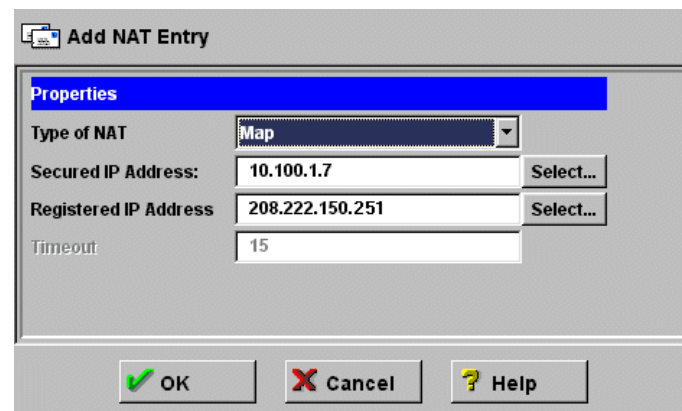


Figure 53. Add NAT Entry

4. Enter the Secure IP Address (POP3 server).
5. Enter the Registered IP Address (208.222.150.251).
6. Click **OK**. The window shown in Figure 54 on page 54 appears.

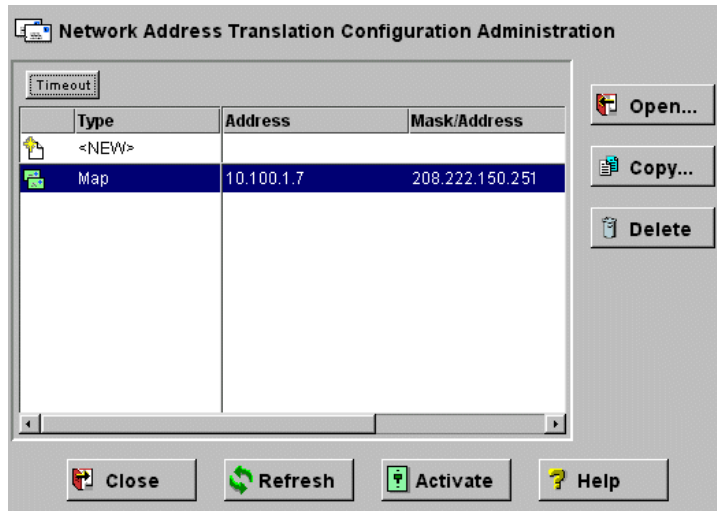


Figure 54. Activate NAT map settings

7. Click **Activate**. The window shown in Figure 55 appears.

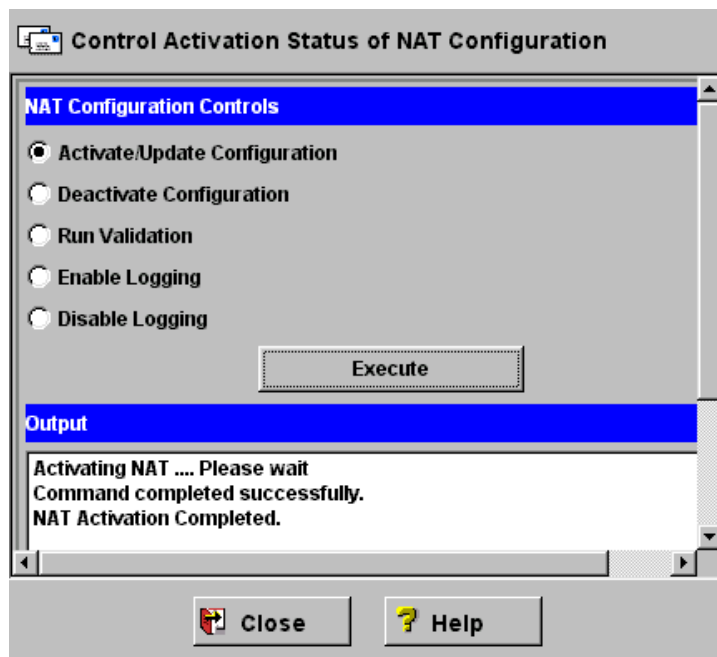


Figure 55. Update NAT configuration

8. Click **Execute**.

9. Verify in the Output window that the operations completed successfully.

3.4.8 Adding new rules

Additional filter rules are necessary for any public server behind the firewall, for example, the POP3 server in our scenario. The following POP3 rules are needed.

Rule 1: Permit inbound POP3 requests

Action:permit, Protocol: tcp, Source port: gt 1023, Destination port: eq 110, Interface non-secure, Routing: route, Direction: inbound, Log: no, Fragment: yes.

Rule 2: Permit outbound POP3 requests

Action:permit, Protocol: tcp, Source port: gt 1023, Destination port: eq 110, Interface secure, Routing: route, Direction: outbound, Log: no, Fragment: yes.

Rule 3: Permit inbound POP3 replies

Action:permit, Protocol: tcp/ack, Source port: eq 110, Destination port: gt 1023, Interface secure, Routing: route, Direction: inbound, Log: no, Fragment: yes.

Rule 4: Permit outbound POP3 replies

Action:permit, Protocol: tcp/ack, Source port: eq 110, Destination port: gt 1023, Interface non-secure, Routing: route, Direction: outbound, Log: no, Fragment: yes.

To create new rules, follow these steps:

1. Double-click **Rules** in the Connections Templates folder in the navigation tree. The window in Figure 56 is displayed.

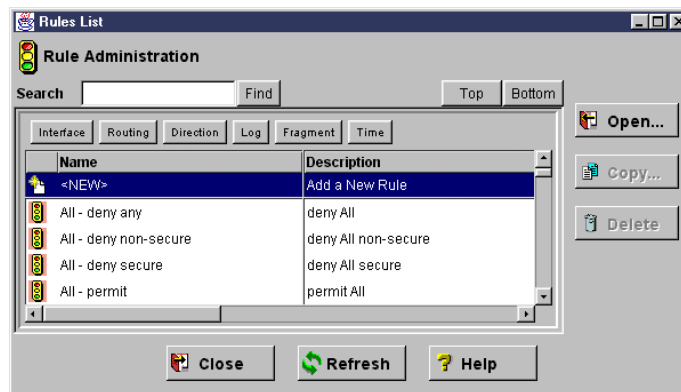


Figure 56. Rule Administration

2. Double-click **NEW**. The window shown in Figure 57 on page 56 appears.

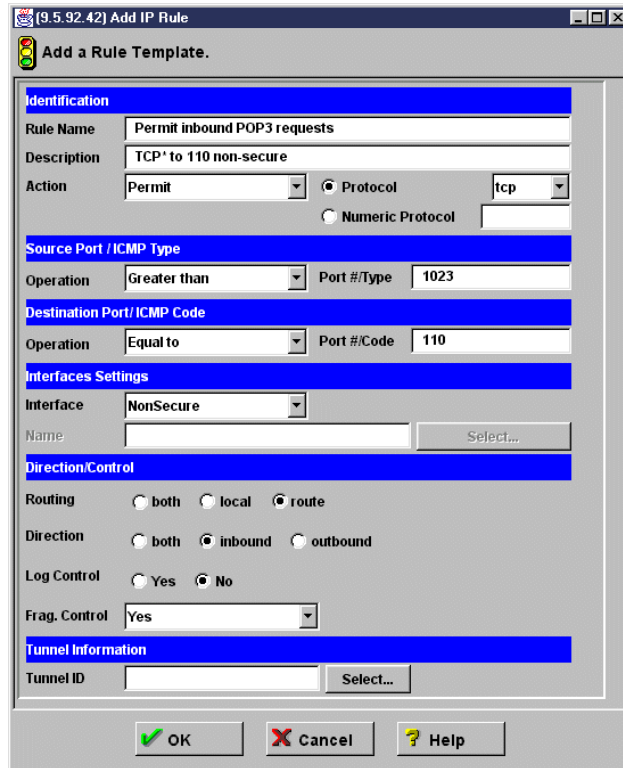


Figure 57. Add a Rule Template

3. Fill in all information about the first rule.
4. Click **OK**.
5. Repeat the steps 3 and 4 for rules 2, 3, and 4.
6. Click **Close**.

3.4.9 Creating a service

To use these rules, a new *service* is needed. A service describes the traffic flow and the order in which the rules are used. To create a new service, follow these steps:

1. Double-click **Services** in the Connections Templates folder in the navigation tree. The window in Figure 58 on page 57 is displayed.

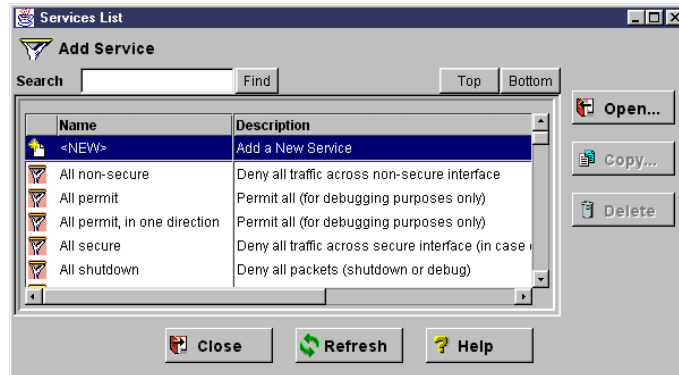


Figure 58. Add Service

2. Double-click **NEW**. The window shown in Figure 59 appears.

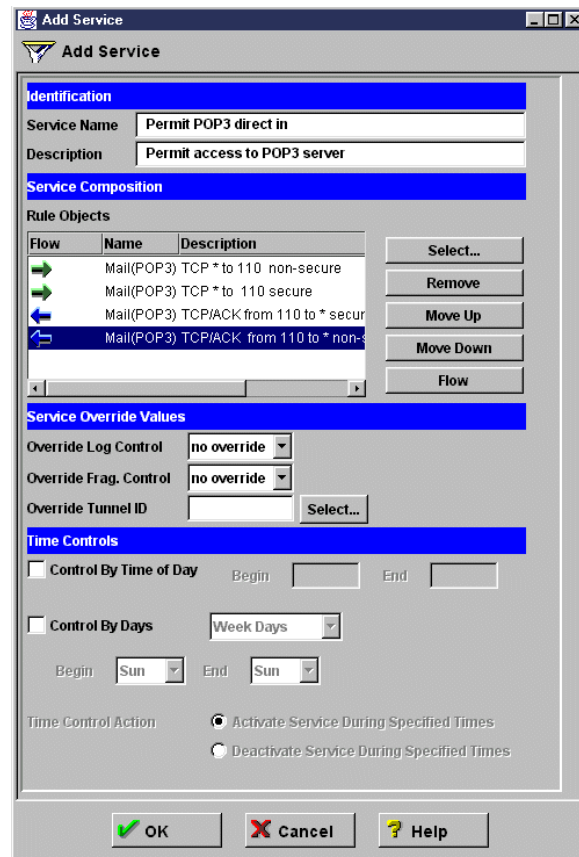


Figure 59. Add Service

3. Click **Select** to choose the four rules in the order that you want them.
4. Select each rule, and click **Flow** to choose the direction of the traffic.
5. Click **OK**.
6. Click **Close**.

3.4.10 Creating a network object

Network objects refer to IP addresses, subnets, or interfaces. In our case, we need to create a network object referred to the internal POP3 server. To create a new network object, follow these steps:

1. Double-click **Network Objects** in the root on the navigation tree. The window in Figure 60 is displayed.

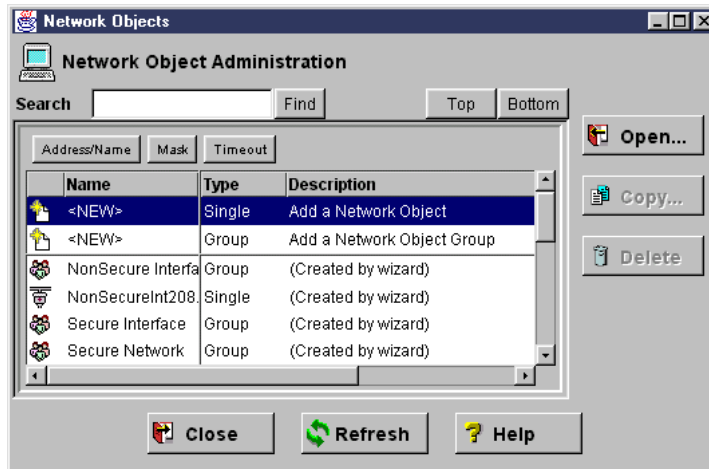


Figure 60. Network Object Administration

2. Double-click **NEW** with Type **Single**. The window shown in Figure 61 appears.

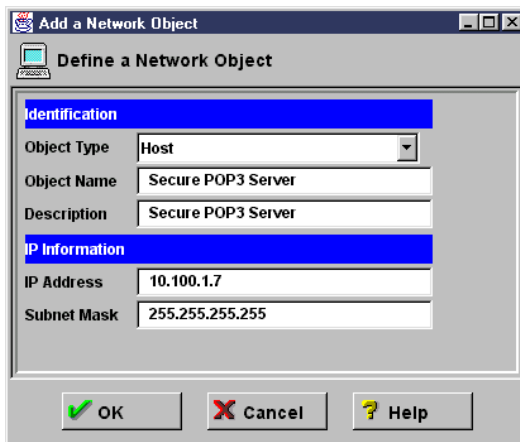


Figure 61. Define a Network Object

3. Choose **Host** for Object Type.
4. Fill in all the information about the secure internal POP3 server.
5. Click **OK**.
6. Click **Close**.

3.4.11 Creating a connection

Basically, a *connection* is a way to associate a *service* to *Network Objects*. To create a new connection, complete these tasks:

1. Double-click **Connections Setup** in the Traffic Control folder in the navigation tree. The window in Figure 62 is displayed.

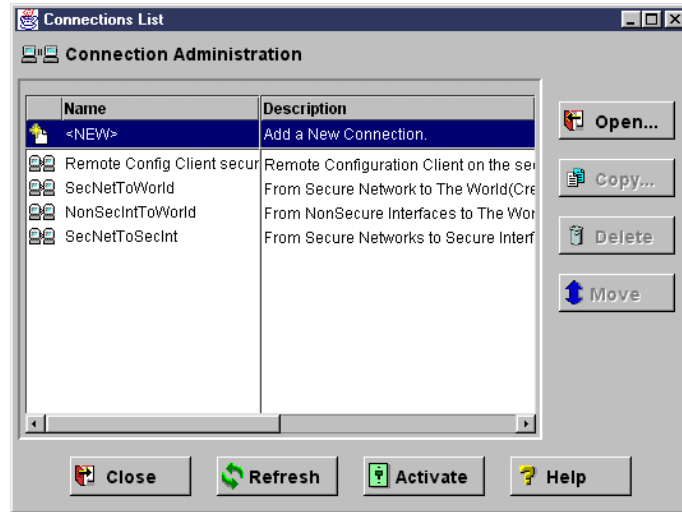


Figure 62. Connection Administration

2. Double-click **NEW**. The window shown in Figure 63 appears.

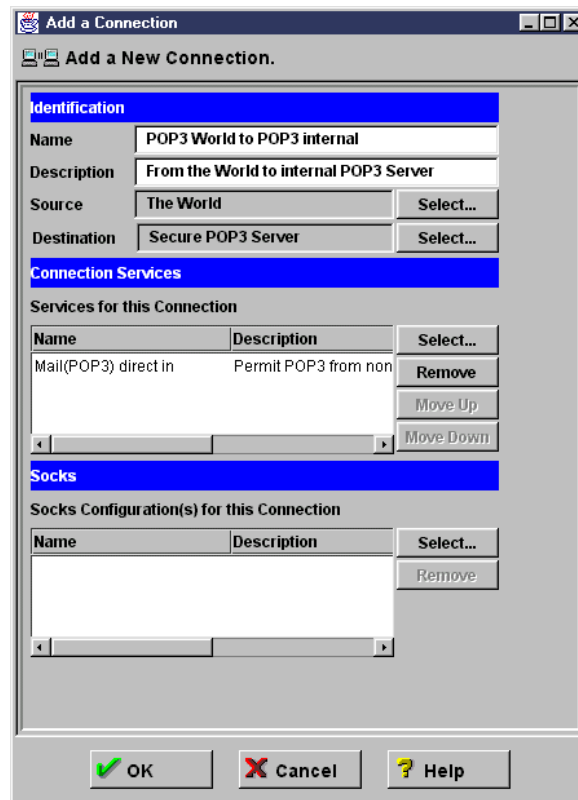


Figure 63. Add a New Connection

3. Select **The World** as the source.
4. Select **Secure POP3 Server** as the destination.
5. Select **Mail POP3 direct in** as the service.

6. Click **OK**.
7. Click **Close**.

3.4.12 Activating rules

Now everything is ready to run your new rules. Before you run your firewall, you *must* verify how the new rules are implemented. Follow these steps:

1. To verify the rules, double-click **Connections Activation** in the Traffic Control folder in the navigation tree. The window in Figure 64 is displayed.

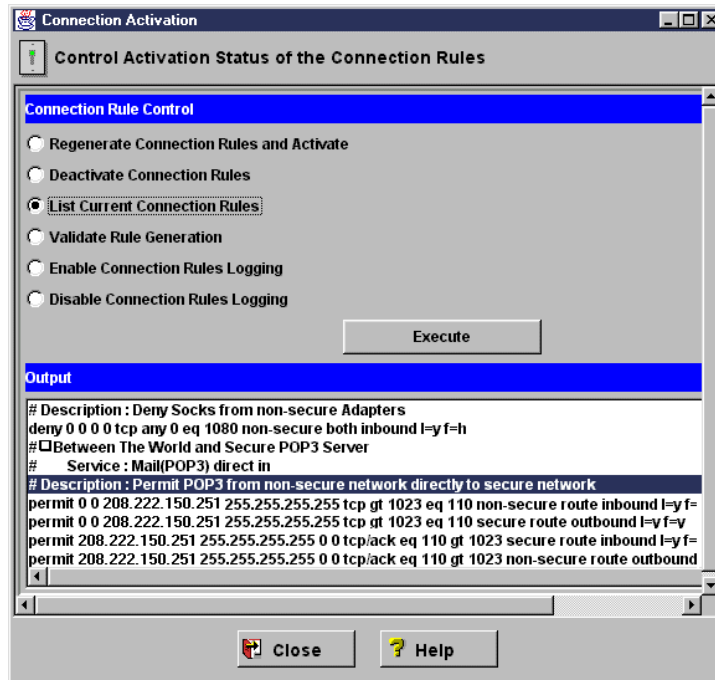


Figure 64. Control Activity Status of the Connection Rules

2. Choose **Validate Rule Generation**.
3. Click **Execute**.
4. If an error occurs, verify each step by of your operation. Do *not* activate your rules. Refer to *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT*, SG24-5209, for more information.
5. If no errors occur, choose **Regenerate Connection Rules and Activate**.
6. Click **Execute**.
7. Your rules must match the following rules:

```

permit 0.0.0.0 208.222.150.251 255.255.255.255 tcp gt 1023 eq 110 non-secure
route inbound l=n f=y (Permit inbound POP3 requests)
permit 0.0.0.0 208.222.150.251 255.255.255.255 tcp gt 1023 eq 110 secure
route outbound l=n f=y (Permit outbound POP3 requests)
permit 208.222.150.251 255.255.255.255 0.0.0.0 tcp/ack eq 110 gt 1023 secure
route inbound l=n f=y (Permit inbound POP3 replies)
permit 208.222.150.251 255.255.255.255 0.0.0.0 tcp/ack eq 110 gt 1023
non-secure route outbound l=n f=y (Permit outbound POP3 replies)

```

3.4.13 Filter rules to allow Domino access from the Internet

Since we are also using a Domino server on HOME400, you may want to open the firewall to give remote Lotus Notes clients access to it. One way for these clients to have access is through the Internet. By default, Domino does not encrypt the data that it sends. Be aware that this data is sent in the clear over the Internet. You may select encryption in the Notes Client.

To enable a Domino client on the untrusted side of the firewall to have access to the Domino server on the secure side of the firewall, you *must* add filter settings. The Domino server listens on port 1352 for Lotus Notes clients.

Use the procedure from 3.4.8, “Adding new rules” on page 55, through 3.4.12, “Activating rules” on page 60, to set up new rules.

Your Domino rules must match the following rules:

```
permit 0.0.0.0 208.222.150.251 255.255.255.255 tcp gt 1023 eq 1352 non-secure
route inbound l=n f=y (Permit non-secure inbound Domino request and
replies)
permit 0.0.0.0 208.222.150.251 255.255.255.255 tcp gt 1023 eq 1352 secure route
outbound l=n f=y (Permit secure outbound Domino request and replies)
permit 208.222.150.251 255.255.255.255 0.0.0.0 tcp eq 1352 gt 1023 secure route
inbound l=n f=y (Permit secure inbound Domino request and replies)
permit 208.222.150.251 255.255.255.255 0.0.0.0 tcp eq 1352 gt 1023 non-secure
route outbound l=n f=y (Permit non-secure outbound Domino request and
replies)
```

Note

This set of rules specifies a port value of 1352, which is different than the other rule sets for this scenario. Also, the first set of rules specifies TCP/ACK in the last two (response) rules, while this set specifies TCP only. By having TCP in the protocol, the Domino server can start TCP/IP sessions, and respond to sessions.

IBM eNetwork Firewall for Windows NT configuration is now ready. For more information about IBM eNetwork Firewall for Windows NT, refer to Appendix D, “Firewall concepts” on page 349.

3.5 Configuring the SMTP server on the AS/400 system

This section describes the tasks that you must perform to install and configure an SMTP to handle one domain with subdomains on a single mail server using a firewall.

3.5.1 Task summary

The following list summarizes the tasks used to implement the SMTP server on the AS/400 HOME400:

1. Set up the SMTP attributes.
2. Verify the HOME400 TCP/IP domain name information.
3. Handle multiple SMTP domains on a single AS/400 system.
4. Add the firewall name to the host table entries.
5. Start the SMTP server.

3.5.2 Setting up SMTP attributes

To route mail for Internet users to the firewall, you *must* configure the SMTP attributes in the AS/400 system to point to the firewall as the mail router. Entering the firewall name in the Mail router field tells the SMTP server where to forward mail that it cannot deliver itself. Complete these tasks:

1. On an AS/400 command line, type:
`CHGSMTPA`
2. Press **F4**, and then Page Down.
3. You *must* enter ***YES** in the Firewall field. This tells the SMTP server that it is located behind a firewall.
4. Enter the correct values, as shown in Figure 65, and press Enter.

```
Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

User ID delimiter . . . . . '?'          *SAME, *DFT, ?, =, ., &, $...
Mail router . . . . . > FW1MAIL.DOMAIN.COM
                               (FW1NT.DOMAIN.COM for the NT firewall)

Coded character set identifier    00819      1-65533, *SAME, *DFT
Mapping tables:
  Outgoing EBCDIC/ASCII table .  *CCSID      Name, *SAME, *CCSID, *DFT
  Library . . . . .                Name, *LIBL, *CURLIB

  Incoming ASCII/EBCDIC table .  *CCSID      Name, *SAME, *CCSID, *DFT
  Library . . . . .                Name, *LIBL, *CURLIB
Firewall . . . . . > *YES          *YES, *NO, *SAME
Journal . . . . . *NO             *YES, *NO, *SAME
Process all mail through MSF . . *NO        *YES, *NO, *SAME
Percent routing character . . .  *YES        *YES, *NO, *SAME
```

Figure 65. Change SMTP Attributes

3.5.3 Verifying the HOME400 TCP/IP domain name information

Enter the Change TCP/IP Domain (`CHGTCPDMN`) command. In the Host name search priority field, type `*LOCAL`. Searching priority `*LOCAL` causes the AS/400 system to look at the host table entries first, before querying the DNS. Figure 66 on page 63 shows the configuration values in the `CHGTCPDMN` command (or `CFGTCP` option 12) screen.

```

Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name . . . . . HOME400

Domain name . . . . . domain.com

Host name search priority . . . *LOCAL      *REMOTE, *LOCAL, *SAME

Internet address . . . . . 10.100.1.7

```

Figure 66. CHGTCPDMN - Search priority *LOCAL

3.5.4 Handling multiple SMTP domains on a single AS/400 system

The objective of this section is to set up the AS/400 system so MFS can recognize that it is listening for the multiple SMTP domain names. In our example, we have three mail domains, referred to as *div1.domain.com*, *div2.domain.com*, and *div3.domain.com*. Each division of the company has its own distinct domain name.

You *must* add three IP addresses and three host table entries for the SMTP mail domain names.

Proceed as follows for each IP address on your AS/400 system:

1. On a command line, type `CFGTCP`. Press **Enter**.
2. Type option 1 to add your TCP/IP address.
3. Type option 10 to add one host table entry.
4. Associate the IP address with the mail domain on the host table entries.

Your host table should appear as shown in Figure 67.

```

Work with TCP/IP Host Table Entries
System: HOME400

Type options, press Enter.
 1=Add  2=Change  4=Remove  5=Display  7=Rename

Internet      Host
Opt  Address   Name

 10.100.1.3   DIV1.DOMAIN.COM
 10.100.1.4   DIV2.DOMAIN.COM
 10.100.1.5   DIV3.DOMAIN.COM
 127.0.0.1    LOOPBACK
              LOCALHOST

```

Figure 67. Associating an IP address with a mail domain

The three IP interfaces do not have to be started. They are only needed because the SMTP server looks on the host table to see for which mail domains it is responsible.

These three IP addresses can also be virtual IP. See Appendix B, “Using virtual IP addresses” on page 329, for further explanation.

Tip

To verify that the AS/400 system is listening for a mail domain on a specific IP address, type `netstat *ifc` on a command line. Then, type `5` in front of the IP addresses you defined. The first line shows the domain associated with the interface.

3.5.5 Adding the firewall name to the host table entries

For the SMTP server to resolve the mail router name defined in the SMTP attributes (Figure 65 on page 62), you *must* configure a host table entry for the firewall.

Specify the **INTERNAL* IP address for IBM Firewall for AS/400 (interface E, Figure 14 on page 28). Specify the secure IP address for IBM eNetwork Firewall for Windows NT (interface B, Figure 27 on page 39).

Figure 68 shows the TCP/IP host table configuration (CFGTCP option 10).

```
Work with TCP/IP Host Table Entries                               System:  HOME400
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  7=Rename

  Internet      Host
  Opt  Address   Name
-----
      192.168.2.2  FW1MAIL
                          FW1MAIL.DOMAIN.COM

(If you use the Windows NT firewall put this entry instead)
      10.100.1.2  FW1NT
                          FW1NT.DOMAIN.COM
```

Figure 68. Firewall configuration on the AS/400 TCP/IP host table

3.5.6 Starting the SMTP server

To start the SMTP server, complete the following tasks:

1. Enter the following command:

```
STRTCPSVR SERVER(*SMTP)
```

2. Use the `WRKACTJOB` command to determine if the mail server framework is running (look in subsystem `QSYSWRK` for jobs named `QMSF`). If the `QMSF` job is not running, use the Start Mail Server Framework (`STRMSSF`) command to start it.

The configuration of the SMTP server is now ready.

3.6 Configuring the POP3 server on the AS/400 system

This section describes the tasks that you must perform to install and configure a POP3 server on the AS/400 HOME400. The POP server is a simple store-and-forward mail system. It provides electronic mailboxes on the AS/400 system from which clients can retrieve mail. It uses the AnyMail/400 mail server framework and the system distribution directory to process and distribute E-mail. It uses simple mail transfer protocol (SMTP) to forward mail.

3.6.1 Task summary

The following list summarizes the tasks used to implement the POP3 server on an AS/400 system:

1. Set up the POP3 server attributes.
2. Configure a default route to route POP3 server responses.
3. Add the POP3 accounts.
4. Configure the POP3 accounts.
5. Start the POP3 server.

3.6.2 Setting up the POP3 server attributes

To set up the POP3 server attributes, complete these tasks:

1. On an AS/400 command line, type:

```
CHGPOPA
```
2. Press **F4**.
3. You *must* enter ***YES** in the Allow standard POP connection field. This tells the POP3 server that you are using a standard POP (TCP/IP) connection. We recommend setting Message split size to ***NOMAX**.
4. Enter the correct values as shown in Figure 69, and press Enter.

```
Change POP Server Attributes (CHGPOPA)

Type choices, press Enter.

Autostart servers . . . . . *YES          *YES, *NO, *SAME
Number of initial servers . . . 3          1-20, *SAME, *DFT
Inactivity timeout . . . . . 600         10-65535 seconds, *SAME, *DFT
Message split size . . . . . *NOMAX      32-2048 kilobytes, *SAME...
MIME CCSID:
  Coded character set identifier 00819     *SAME, *DFT, 00819, 00912...
  When to use . . . . . *BESTFIT        *SAME, *BESTFIT, *ALWAYS
Allow standard POP connection . *YES      *SAME, *YES, *NO
Host server connection . . . . *NONE    *SAME, *NONE, *ALL, *IP...
      + for more values
Address book:
  Enabled . . . . . *NO                 *SAME, *NO, *YES
  Refresh interval . . . . .           1-65535 minutes, *NONE
```

Figure 69. Change POP server attributes

3.6.3 Configuring a default route to route POP3 server responses

Because your POP3 server is on the secure side of the firewall, and you have clients accessing from the non-secure network, you *must* configure a default

route pointing to the firewall. This allows POP3 clients in the Internet to receive responses from the internal server.

Specify the **INTERNAL* IP address for IBM Firewall for AS/400 (interface E, Figure 14 on page 28) as the next hop. Specify the internal secure IP address for IBM eNetwork Firewall for Windows NT (interface B, Figure 27 on page 39) as the next hop.

On an AS/400 command line, type:

```
CFGTCIP
```

Select option **2** to update the routes.

```
Work with TCP/IP Routes
System: HOME400
Type options, press Enter.
 1=Add  2=Change  4=Remove  5=Display

Route      Subnet      Next      Preferred
Opt  Destination  Mask      Hop      Interface

*DFTRROUTE *NONE      192.168.2.2 *NONE

(If you use the Windows NT firewall put this entry instead)
*DFTRROUTE *NONE      10.100.1.2  *NONE
```

Figure 70. TCP/IP default route configuration

3.6.4 Adding POP3 accounts

If your POP3 users are already AS/400 users, skip to 3.6.5, “Configuring POP3 accounts” on page 67. Complete these steps:

1. To create a new user profile, on an AS/400 command line, type:

```
CRTUSRPRF
```

2. Press **F4**.

For security reasons, you may use the INLMNU (*SIGNOFF) parameter. This means that the user is not allowed to sign on to the AS/400 system.

3. Enter the correct values for the user. Use Figure 71 on page 67 as a guide. After you enter the correct values, press Enter.

```

                                Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . .      gaelle           Name
User password . . . . .    *****         Name, *USRPRF, *NONE
Set password to expired . . . . . *NO          *NO, *YES
Status . . . . .           *ENABLED      *ENABLED, *DISABLED
User class . . . . .       *USER         *USER, *SYSOPR, *PGMR...
Assistance level . . . . . *SYSVAL       *SYSVAL, *BASIC, *INTERMED...
Current library . . . . .  *CRIDFT       Name, *CRIDFT
Initial program to call . . . . . *NONE        Name, *NONE
  Library . . . . .        Name, *LIBL, *CURLIB
Initial menu . . . . .     *SIGNOFF    Name, *SIGNOFF
  Library . . . . .        *LIBL          Name, *LIBL, *CURLIB
Limit capabilities . . . . . *NO          *NO, *PARTIAL, *YES
Text 'description' . . . . . 'Gaelle Jenni - POP3 account'

```

Figure 71. Creating a POP3 account

3.6.5 Configuring POP3 accounts

To configure a POP3 account on an AS/400 system, add an entry in the system distribution directory for each user. For users who do *not* have a directory entry, follow these steps:

1. On an AS/400 command line, type:

```
WRKDIRE
```

Press Enter. The display shown in Figure 72 appears.

```

                                Work with Directory Entries

Type options, press Enter.
  1=Add      2=Change  4=Remove  5=Display details  6=Print details
  7=Rename   8=Assign different ID to description  9=Add another description

Opt  User ID  Address  Description
  1
    *ANY      HOME400  Generic entry for HOME400
    DHQB      HOME400  operations userid
    FSTEELE   HOME400  Fant Steele
    QDFTOWN   QDFTOWN   Default Owner
    QDOC      QDOC      Internal Document Owner
    QLPAUTO   QLPAUTO   Licensed Program Automatic User
    QLPINSTL  QLPINSTL  Licensed Program Install
    QNOTES    QNOTES    LOTUS NOTES INTEGRATION PROFILE
    QSECOFR   QSECOFR   Security Officer

```

Figure 72. Work with directory entries

2. Type 1, and then press Enter. The display shown in Figure 73 on page 68 appears. In this document, we include only the relevant parameters in Figure 73, Figure 74, and Figure 75 on page 68.

```

                                Add Directory Entry

Type choices, press Enter.

User ID/Address . . . . . GAELLE    HOME400
Description . . . . .   Gaelle Jenni - POP3 Account
System name/Group . . . . HOME400          F4 for list
User profile . . . . .   GAELLE          F4 for list
Network user ID . . . . .

```

Figure 73. Add Directory Entry (Part 1 of 2)

3. Press the Page Down key three times, or until you arrive at the display shown in Figure 74.

```

                                Add Directory Entry

Type choices, press Enter.

Mail service level . . . 2

                                1=User index
                                2=System message store
                                4=Lotus Domino
                                9=Other mail service

For choice 9=Other mail service:
Field name . . . . . F4 for list

Preferred address . . . 3

                                1=User ID/Address
                                2=O/R name
                                3=SMTP name
                                9=Other preferred address
                                F4 for list

Address type . . . . .
For choice 9=Other preferred address:
Field name . . . . . F4 for list

```

Figure 74. Add Directory Entry (Part 2 of 2)

4. Enter the values shown in Figure 74. Press **F19** (Add name for SMTP). The display shown in Figure 75 appears.

```

                                Change Name for SMTP

User ID/Address . . . . . : GAELLE    HOME400          System: HOME400

Type choices, press Enter.

SMTP user ID . . . . .   gaelle
SMTP domain . . . . .   div1.domain.com

SMTP route . . . . .

```

Figure 75. Adding an SMTP user ID and domain

5. Fill in the SMTP user ID and SMTP domain fields. These values are combined to form the SMTP e-mail address for this user (gaelle@domain1.com). Press Enter.
6. To confirm your choice, press Enter again.

For users who *have* a directory entry, follow these steps:

1. On an AS/400 command line, type:

```
WRKDIRE
```

Press Enter. The display shown in Figure 76 appears.

```

                                Work with Directory Entries

Type options, press Enter.
  1=Add      2=Change  4=Remove  5=Display details  6=Print details
  7=Rename   8=Assign different ID to description  9=Add another description

Opt  User ID  Address  Description
-----
      *ANY    HOME400  Generic entry for HOME400
      DHQB    HOME400  operations userid
      FSTEELE HOME400  Fant Steele
  2   GAELLE  HOME400  Gaelle Jenni - POP3 Account
      QDFTOWN QDFTOWN  Default Owner
      QDOC    QDOC     Internal Document Owner
      QLPAUTO QLPAUTO  Licensed Program Automatic User
      QLPINSTL QLPINSTL Licensed Program Install

```

Figure 76. Work with Directory Entries

2. Type 2, and then press Enter. The display shown in Figure 77 appears. In this redbook, we include only the relevant parameters in Figure 77 and Figure 78 on page 70.

```

                                Change Directory Entry

User ID/Address . . . . . : GAELLE    HOME400

Type changes, press Enter.

Description . . . . .      Gaelle Jenni - POP3 account
System name/Group . . . . HOME400                      F4 for list
User profile . . . . .    GAELLE      F4 for list
Network user ID . . . . . GAELLE    HOME400

                                                                More...
```

Figure 77. Change Directory Entry (Part 1 of 2)

3. Press the Page Down key four times, or until you arrive at the display, which is shown in Figure 78 on page 70.

```

Change Directory Entry
User ID/Address . . . . . : GAELLE      HOME400

Type changes, press Enter.

Mail service level . . . 2
                            1=User index
                            2=System message store
                            4=Lotus Domino
                            9=Other mail service

For choice 9=Other mail service:
Field name . . . . .      F4 for list

Preferred address . . . . 3
                            1=User ID/Address
                            2=O/R name
                            3=SMTP name
                            9=Other preferred address
                            F4 for list

Address type . . . . .
For choice 9=Other preferred address:
Field name . . . . .      F4 for list
More...

```

Figure 78. Changing Directory Entry (Part 2 of 2)

4. Enter the values shown in Figure 78. Press **F19** (Add name for SMTP). The display shown in Figure 79 appears.

```

Change Name for SMTP
User ID/Address . . . . . : GAELLE      HOME400
System: HOME400

Type choices, press Enter.

SMTP user ID . . . . .    gaelle
SMTP domain . . . . .    div1.domain.com

SMTP route . . . . .

```

Figure 79. Adding an SMTP user ID and domain

5. Fill in the SMTP user ID and SMTP domain fields. These values are combined to form the SMTP e-mail address for this user (gaelle@div1.domain.com). Press Enter.
6. To confirm your choice, press Enter again.

3.6.6 POP3 mailboxes

Once there is an entry in the system distribution directory for a POP mail user, the mailbox for that user is created automatically, either the first time the client logs on successfully or when mail is received for the client.

3.6.7 Starting the POP3 server

To start the POP3 server, complete the following tasks:

1. Enter the following command:

```
STRTCPSVR SERVER(*POP)
```

2. Use the `WRKACTJOB` command to determine if the mail server framework is running (look in subsystem QSYSWRK for jobs named QMSF). If the QMSF job is not running, use the Start Mail Server Framework (`STRMSF`) command to start it.

The configuration of the POP3 server is now ready.

3.7 Configuring the Domino server for mail

This section describes the tasks that you must perform to configure a Domino server to handle multiple domains using a firewall.

3.7.1 Task summary

The following list summarizes the tasks used to implement the Domino server on the AS/400 HOME400:

1. Plan the Domino server on an AS/400 system.
2. Set up HOME400 to handle Domino.
3. Install the Domino server on HOME400.
4. Install Domino Administrator on your workstation.
5. Set up your workstation to administer Domino.
6. Configure Domino server for SMTP mail.
7. Link the Domino server with the firewall.
8. Create Lotus Notes mail users.

3.7.2 Planning the Domino server on an AS/400 system

There are several ways to implement a Domino server on an AS/400 system to handle SMTP mail:

- SMTP server on the Domino server
- SMTP server with MSF on the AS/400 system
- SMTP server with MSF on the AS/400 system and Domino server

The first configuration, SMTP server on the Domino server, is the one we implement in this scenario. The second configuration, SMTP server with MSF on the AS/400 system, is documented in 5.9, "Configuring Domino with MSF on the AS/400 system" on page 183.

The third possibility needs specific configurations. If you need to use both the SMTP server on the AS/400 system and the SMTP server on the Domino server, you have to bind each application to a specific IP address. Refer to the Dual Stack PTF cover letter. In V4R2, this is supported by PTF SF55697. In V4R3, this is supported by PTF SF58661. A PTF is under development for V4R4. These PTFs are OS/400 PTFs that are used to add the feature. The cover letter for the PTF also lists a corresponding co-requisite PTF from the POP snap-ins.

3.7.3 Setting up HOME400 to handle Domino

To use Domino on an AS/400 platform, we strongly recommended that you add a unique TCP/IP address for each Domino server. Follow these steps:

1. On an AS/400 command line, type:

```
ADDTCPIFC F4.
```

The display shown in Figure 80 appears.

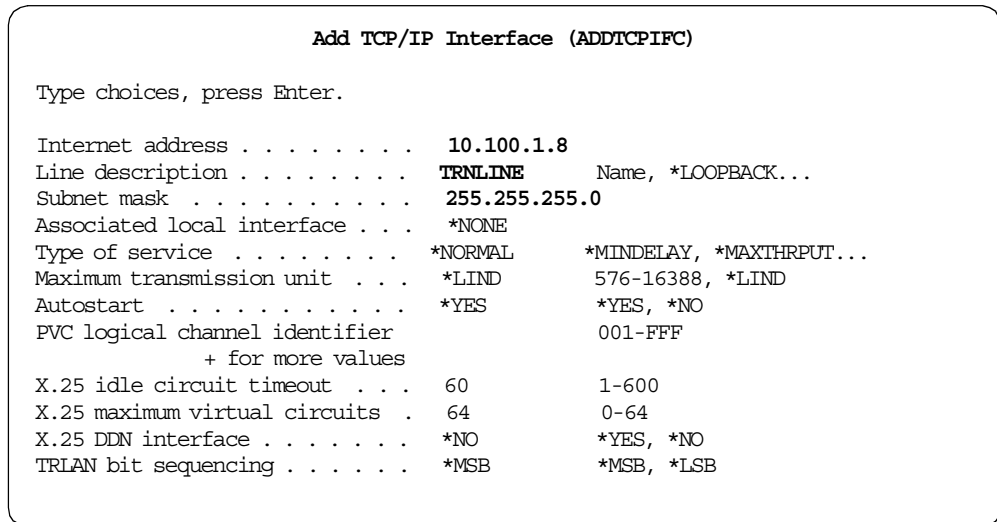


Figure 80. Add TCP/IP Interface

2. Enter the IP address, line description, and subnet mask.
3. Press Enter.
4. Start the IP interface by typing 9 beside the IP address.

You successfully added a TCP/IP interface to your AS/400 system. This IP address can also be a virtual IP address. See Appendix B, "Using virtual IP addresses" on page 329, for further explanation.

3.7.4 Installing Domino server on HOME400

Install the Domino server using the instructions in *Lotus Domino for AS/400 R5: Implementation*, SG24-5592. If you do not have this redbook or do not have Internet access to download it, you can review the parameters shown in Figure 81 on page 73 through Figure 84 on page 74:

1. Insert the CD-ROM Lotus Domino for AS/400.
2. Install the product using the command:

```
LODRUN DEV(*OPT) DIR('/OS400')
```

3. On a AS/400 command line, type:

```
CFGDOMSVR F4
```



```

                                Configure Domino Server (CFGDOMSVR)

Type choices, press Enter.

Server name . . . . . > DOM400

Option . . . . . > *FIRST          *FIRST, *ADD, *REMOVE
Data directory . . . . . > '/DOMINO/DOM400/DATA'

Organization . . . . . > DOMAIN

```

Figure 81. Configure Domino Server (Part 1 of 4)

```

                                Configure Domino Server (CFGDOMSVR)

Type choices, press Enter.

Administrator:
  Last name . . . . . > Remy

  First name . . . . . > Gagnebin
  Middle initial . . . . .                                     Character value
  Password . . . . . > lartisan
  Minimum password length . . . 8                             0-31
  Internet password . . . . . *NONE
  Time zone . . . . . > CST                                   GMT, EST, CST, MST, PST, CET ...
  Daylight savings time . . . . > *NO                       *YES, *NO
  Web browsers . . . . . > *NONE                             *NONE, *ALL, *HTTP, *IIOP

  Internet mail packages . . . . > *SMTP                    *NONE, *ALL, *IMAP, *POP3 ...
    + for more values
  SMTP services . . . . . *DOMINO                           *DOMINO, *MSF

```

Figure 82. Configure Domino Server (Part 2 of 4)

```

                                Configure Domino Server (CFGDOMSVR)

Type choices, press Enter.

Directory services . . . . . *NONE                          *NONE, *ALL, *SYSDIR, *LDAP

News readers . . . . . *NONE                                *NONE, *NNTP
Connection services . . . . . *DECS                        *DECS, *NONE
Advanced services . . . . . *NONE                          *NONE, *ALL, *PARTITION...
    + for more values

                                Additional Parameters

Replace configuration . . . . . *YES                        *YES, *NO
Domain name . . . . . *ORG
Network name . . . . . NETWORK1
Country code . . . . . > *BLANK
Certifier ID . . . . . *GEN

```

Figure 83. Configure Domino Server (Part 3 of 4)

```

Configure Domino Server (CFGDOMSVR)

Type choices, press Enter.

Administrator ID . . . . . *GEN

Server ID . . . . . *GEN

Start server . . . . . *YES      *YES, *NO
Log replication events . . . . . *YES      *YES, *NO
Log client session events . . . . *YES      *YES, *NO
TCP/IP port options:
  Encrypt network data . . . . . *NOENCRYPT *ENCRYPT, *NOENCRYPT
  Internet address . . . . . > '10.100.1.8'
Subsystem and object names . . . *GEN      Name, *GEN
Collation . . . . . *STD      *STD, CS, DA-DK-AA, DE, E2-ES ...
Copy Administrator ID file . . . *ALL      *DOMDIR, *DTADIR, *ALL
Additional services . . . . . *NONE      *NONE, *ICM
      + for more values

```

Figure 84. Configure Domino Server (Part 4 of 4)

3.7.5 Installing Domino Administrator on your workstation

Install the Lotus Domino Administrator program by following these steps:

1. Insert the Domino 5 client CD in your computer.
2. Run the Domino 5 client setup program.
3. During the installation, select **All clients** (Lotus Notes, Domino Administrator, and Domino Designer). This provides additional functions that can be used for design and testing. The minimum requirement is to install the Domino Administrator.
4. Restart your computer.

Configure the Domino Administrator program:

5. To start the configuration, choose **Lotus Domino Administrator** in the **Lotus Applications** folder. The window shown in Figure 85 on page 75 appears. Read the window carefully.

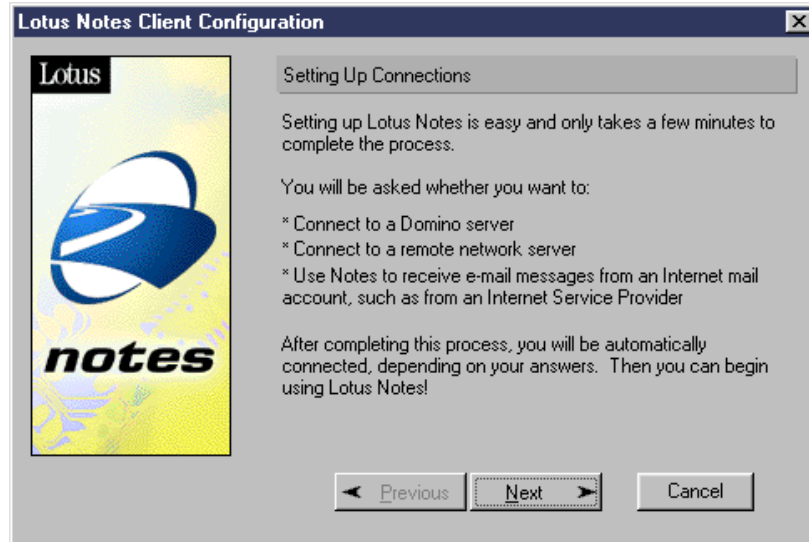


Figure 85. Lotus Notes Client Configuration - Setting up connections

6. Click **Next**. The window shown in Figure 86 appears.

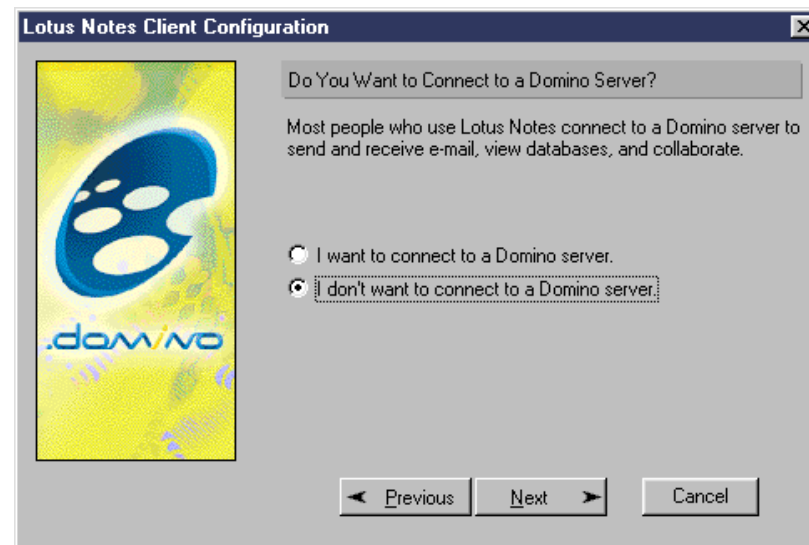


Figure 86. Lotus Notes Client Configuration - Connecting to a Domino server

7. Select **I don't want to connect to the Domino server now**.

8. Click **Next**. The window shown in Figure 87 on page 76 appears.

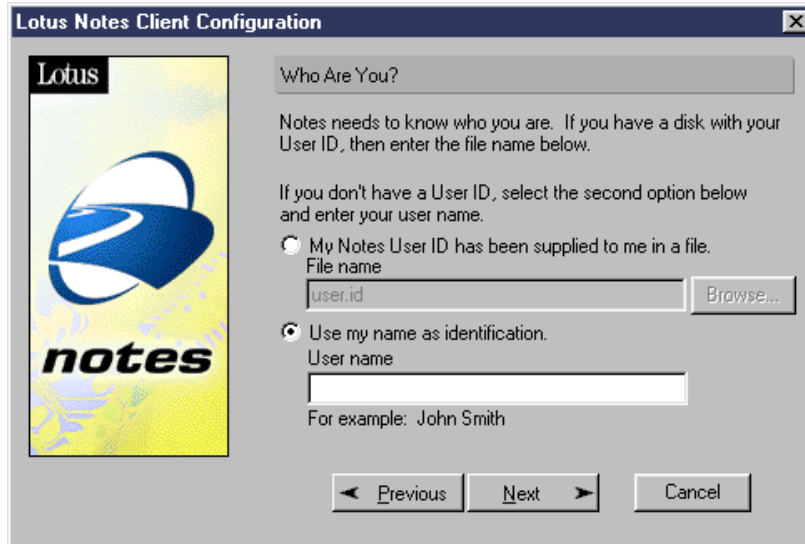


Figure 87. Lotus Notes Client Configuration - User ID

9. Enter your user name, as defined in the CFGDOMSVR command (Figure 82 on page 73).
10. Click **Next**. The window shown in Figure 88 appears.

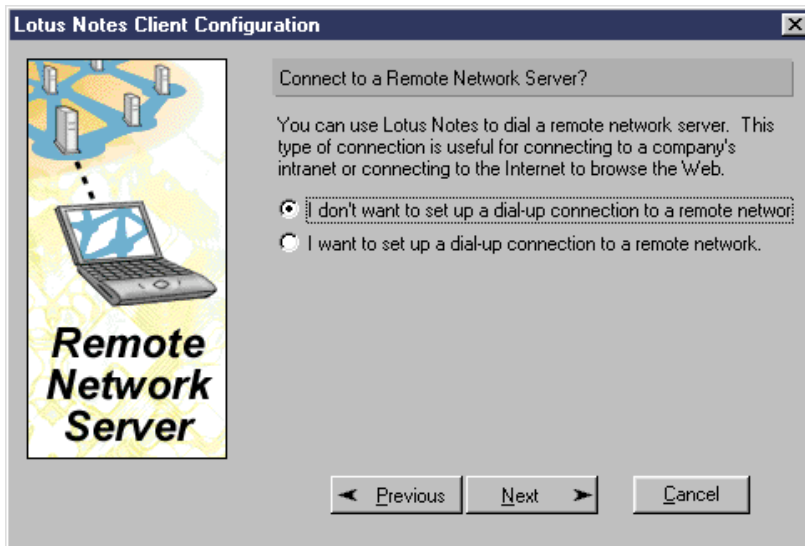


Figure 88. Lotus Notes Client Configuration - Connecting to a remote server

11. Select the option **I don't want to set up a dial-up connection to a remote network**.
12. Click **Next**. The window shown in Figure 89 on page 77 appears.



Figure 89. Lotus Notes Client Configuration - Setting up an Internet mail account

13. Select the option **I don't want to create an Internet mail account.**

14. Click **Next**. The window shown in Figure 90 appears.

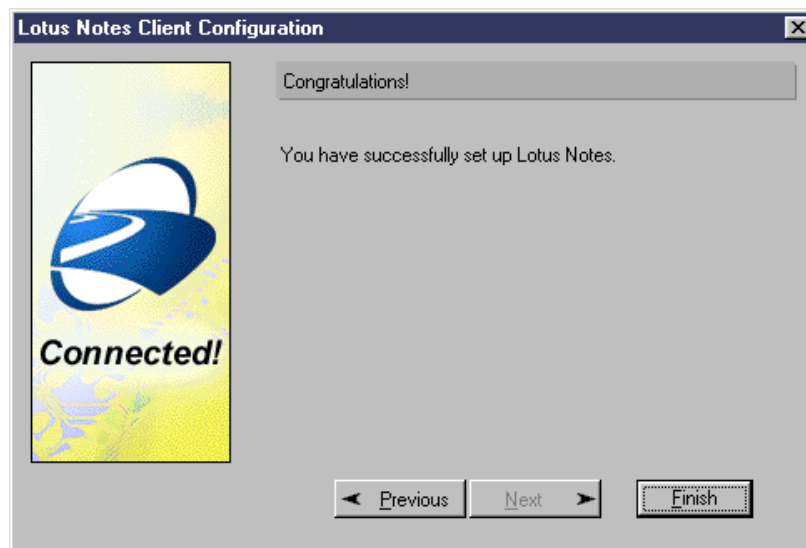


Figure 90. Lotus Notes Client Configuration - Finish

15. Click **Finish**. The Domino Administrator desktop appears, as shown in Figure 91 on page 78.



Figure 91. Lotus Domino Administrator desktop

You successfully configured the Domino Administrator program.

3.7.6 Setting up your workstation to administer Domino

This is the way to set up the Lotus Domino Administrator program to administer a Domino server. During the first step, we rename the USER.ID and CERT.ID. We do this because, in the future, you may want to manage more than one Domino server. Renaming your CERT.ID and USER.ID files makes your IDs easier to understand.

1. Copy the USER.ID and CERT.ID on your workstation directory. One way to do this is by following these steps:
 - a. Open an MS-DOS session on your workstation.
 - b. Start FTP by typing: `FTP home400.domain.com`
 - c. Enter your AS/400 user ID and AS/400 password.
 - d. Type `bin` to change the representation type to *binary image*.
 - e. Type `quote site namefmt 1` to change the naming format.
 - f. Type `cd /domino/dom400/data` as specified in the Configure Domino Server (CFGDOMSVR) command.
 - g. Type `lcd c:\notes\data\ids\people`
 - h. Type `get user.id admin_dom400.id`
 - i. Type `lcd c:\notes\data\ids\certs`
 - j. Type `get cert.id domain.id`
 - k. Type `quit` to end the FTP session.
 - l. Close the MS-DOS prompt window by typing `exit`

If your Domino server name is not in your DNS server and your workstation host table does not already contain the Domino server name, you have to add the information now. Lotus Domino Administrator needs the information when it performs name resolution. You may also add a connection document for the Domino Server. Adding a connection document is not covered here.

2. Open the Lotus Domino Administrator program, choose the **File** menu, select **Mobile**, and then select **Location**. The window shown in Figure 92 appears.

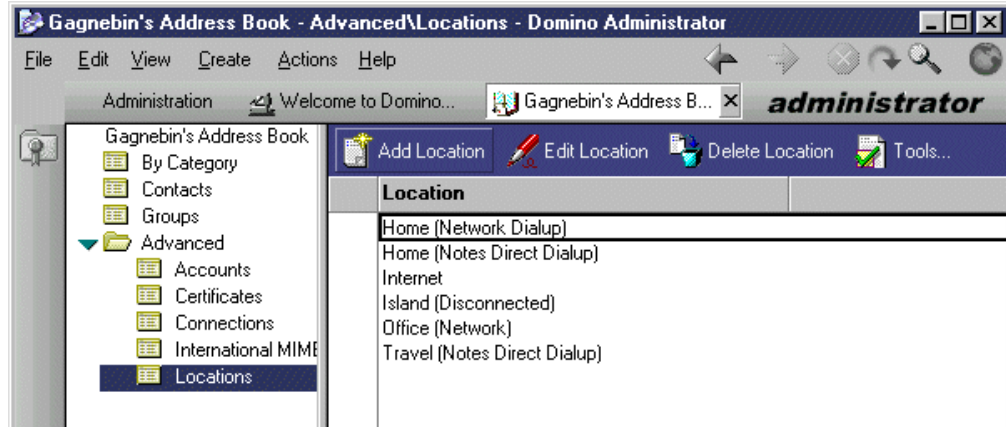


Figure 92. Adding a location

3. Click the **Add Location** icon. The window shown in Figure 93 appears.

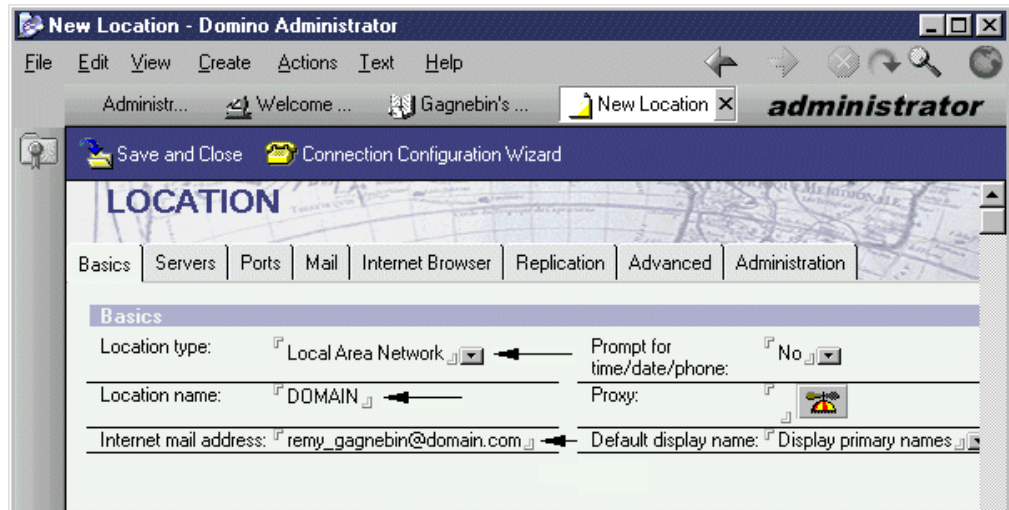


Figure 93. Location document - Basics

4. Choose **Local Area Network** as Location type.
5. Enter the Location name as `DOMAIN` (it can be any name).
6. Enter your Internet mail address.
7. Click the **Servers** tab. The window shown in Figure 94 on page 80 appears.

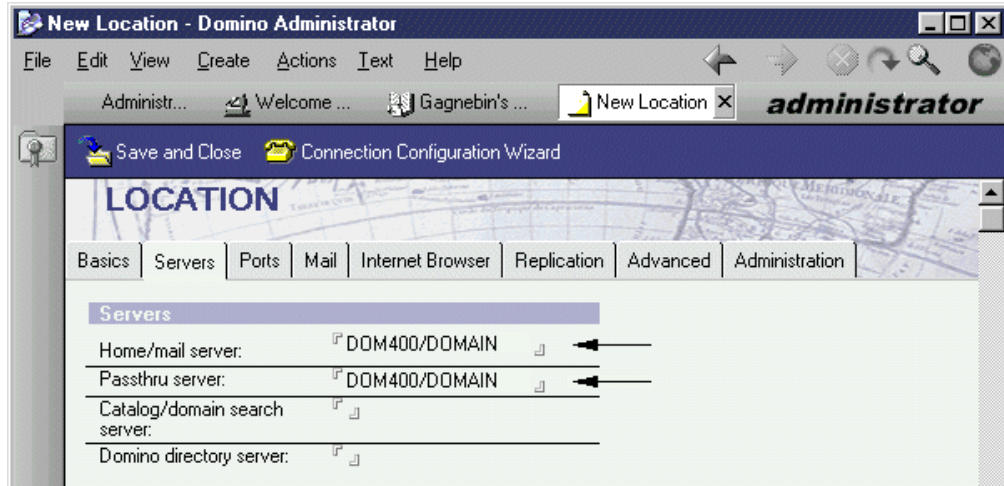


Figure 94. Location document - Servers

8. For the Home/mail server, enter `DOM400/DOMAIN`
9. For the Passthru server, enter `DOM400/DOMAIN`
10. Click the **Mail** tab. The window shown in Figure 95 appears.

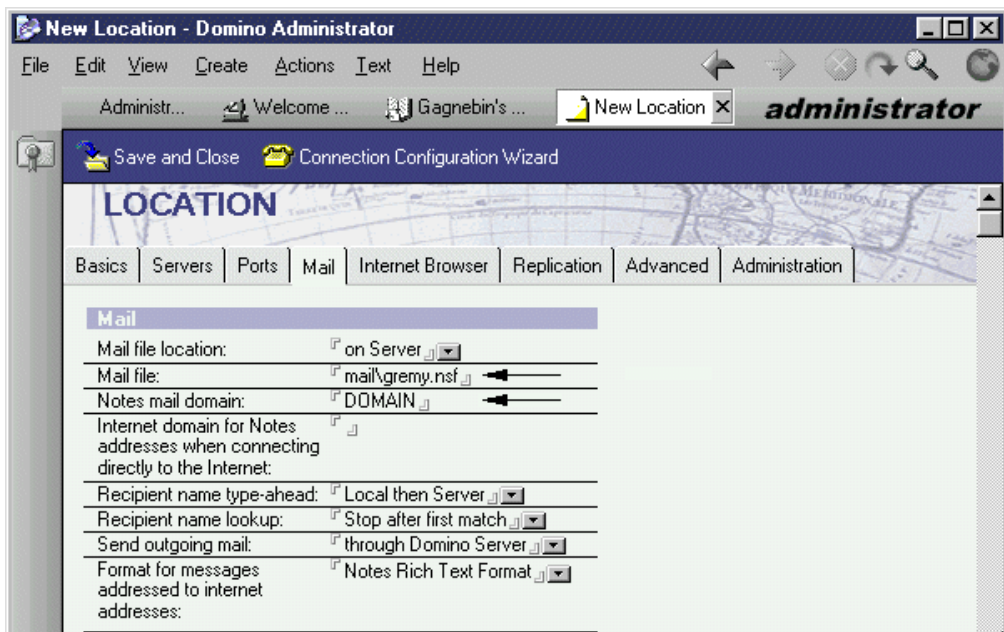


Figure 95. Location document - Mail

11. For the Mail file, enter `mail\gremy.nsf` (path on the server).
12. For the Notes mail domain, enter `DOMAIN`
13. Click the **Advanced** tab. The window shown in Figure 96 on page 81 appears.

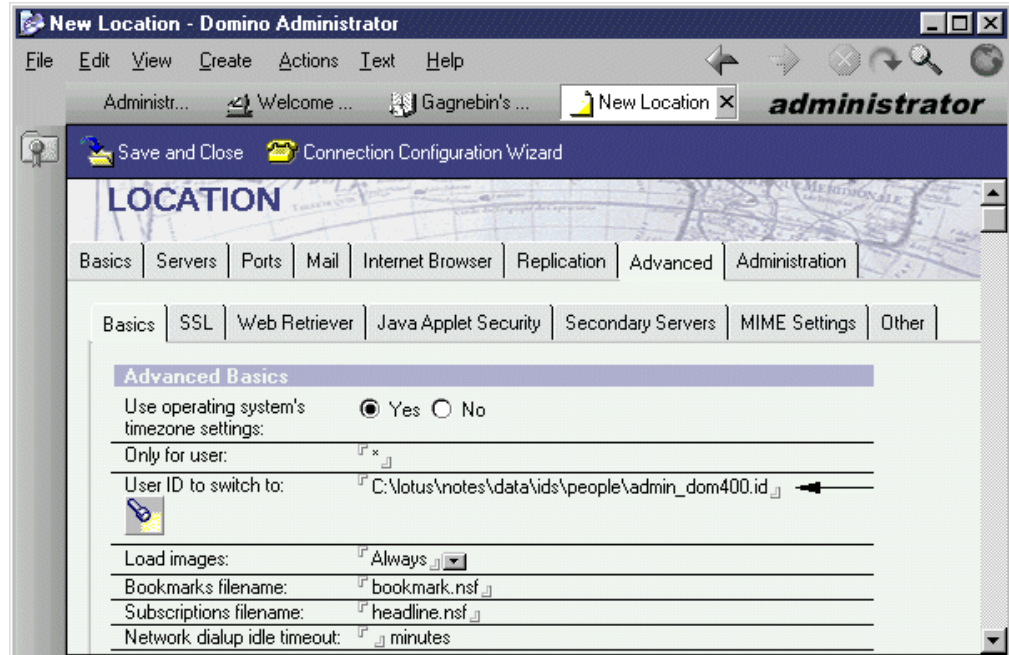


Figure 96. Location document - Advanced

14. Enter the user ID to switch to: c:\...\admin_dom400.id

15. Click **Save and Close**.

You successfully created the Location document.

Complete the following process to access your server:

1. Click the Location pop-up menu, (1) in Figure 97, and choose **DOMAIN**.
2. Enter your password in the prompt window.
3. Click the **Administration** button on the desktop (2). The tabbed pages shown in Figure 97 appear.

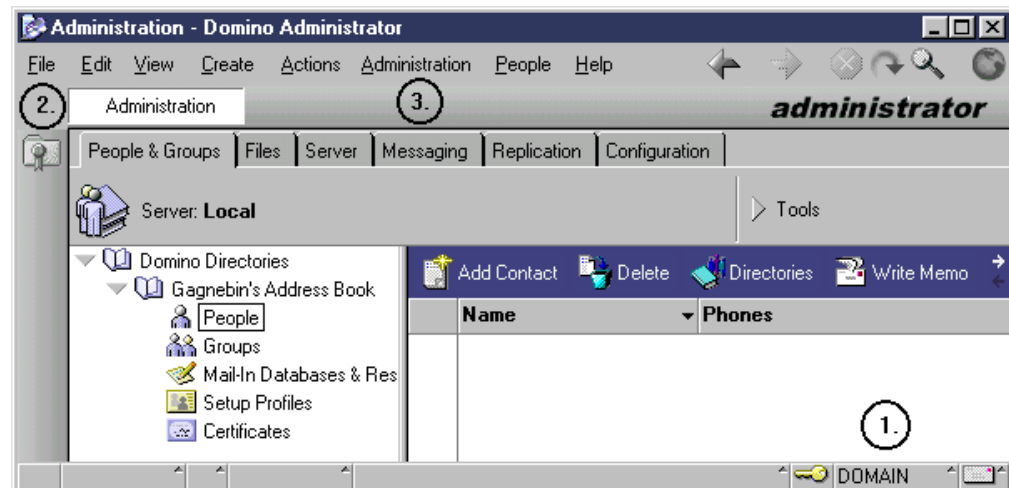


Figure 97. Selecting your location document

4. Choose the **Administration** menu (3), and select **Add server to favorites**. The display shown in Figure 98 appears.

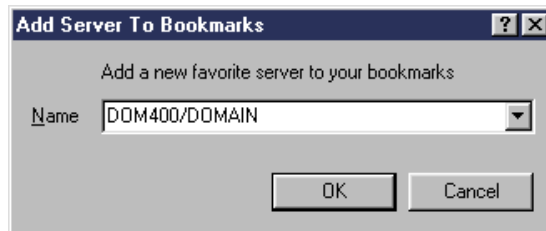


Figure 98. Server Bookmark

5. Enter `DOM400/DOMAIN` as your Domino server name. Click **OK**.
6. On your desktop, click the **Favorites** icon.
7. Choose the server you want to administer as shown in Figure 99.

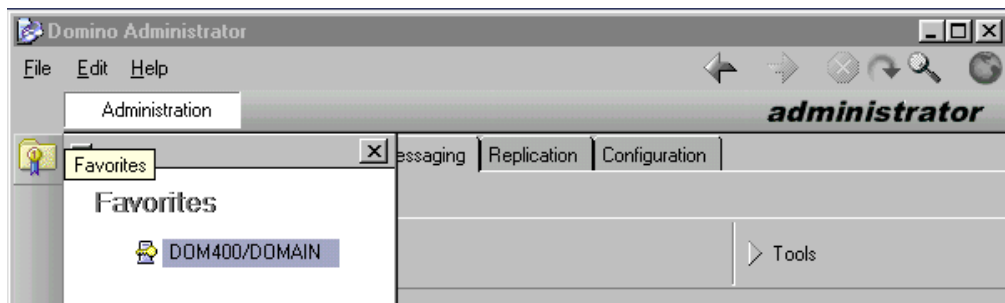


Figure 99. Favorites window

You are now ready to administer your Domino server.

Stop here

If you were referred to this procedure from another chapter in the book, you should return there now.

3.7.7 Configuring Domino server for SMTP mail

This section describes how to set up the Domino server to handle SMTP mail. On the Domino Administrator desktop, execute the following steps. Use the example shown in Figure 100 on page 83 as a guide for the first five steps.

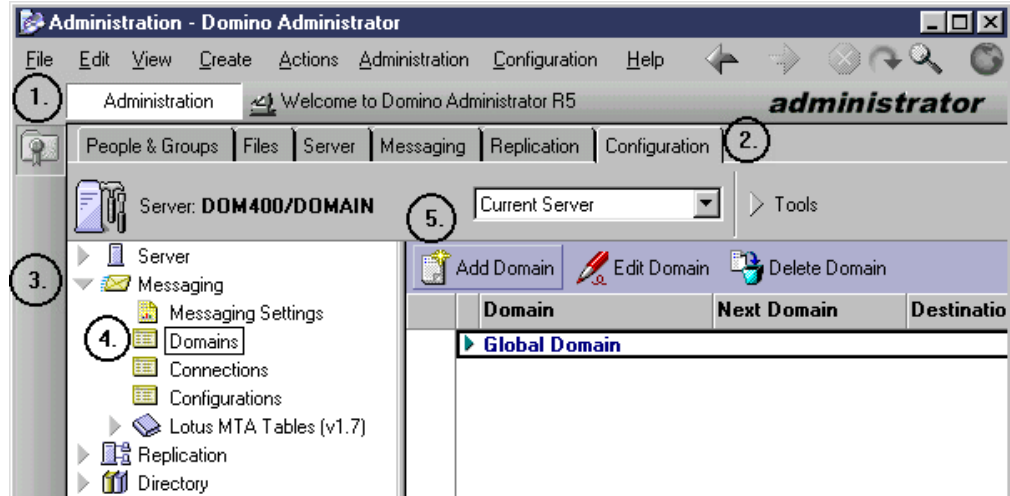


Figure 100. Domain document

1. Click the **Administration** button (1).
2. Click the **Configuration** tab (2).
3. Open **Messaging** in the navigation tree (3).
4. Click **Domains** (4).
5. Click the **Add Domain** button (5). The display shown in Figure 101 appears.

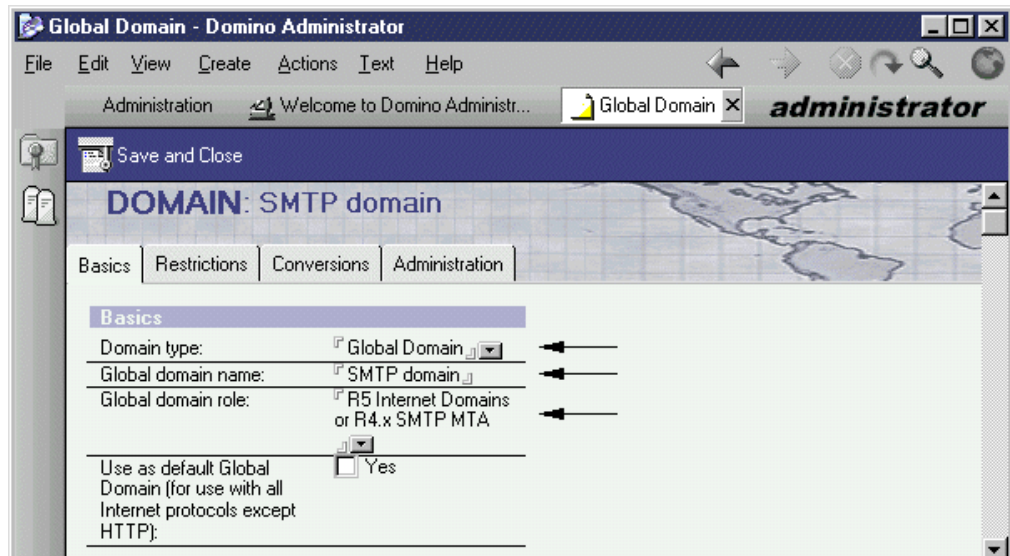


Figure 101. Domain document - Basics

6. Select **Global Domain** for Domain type.
7. Enter **SMTP Domain** for Global domain name.
8. Select **R5 Internet Domains** for Global domain role.
9. Click on the **Conversions** tab. The window shown in Figure 102 on page 84 appears.

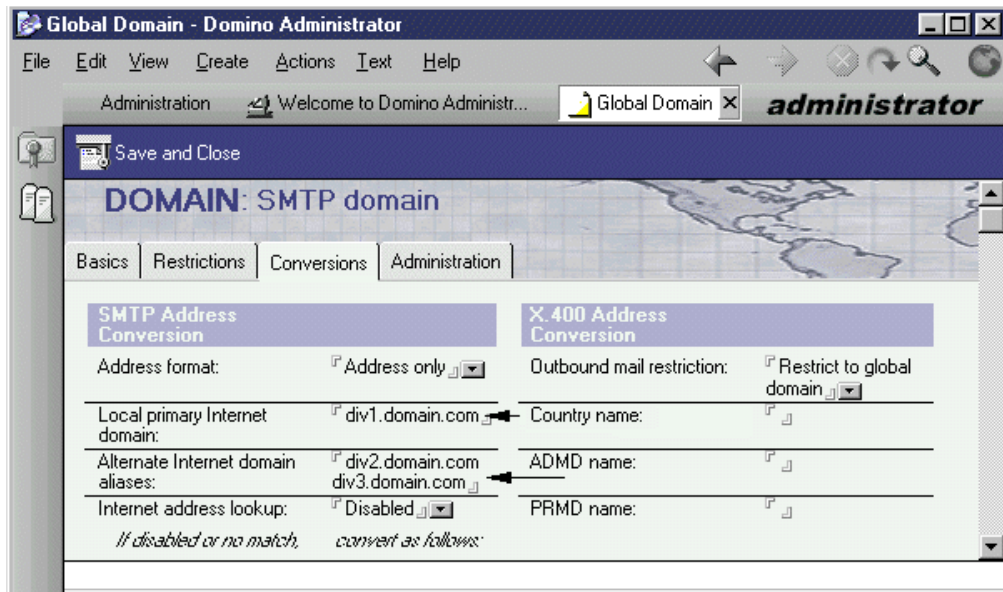


Figure 102. Domain document - Conversion

10. Enter `div1.domain.com` for Local primary Internet domain.
11. Enter `div2.domain.com` and `div3.domain.com` for Alternate Internet domain aliases.
12. Click **Save and Close**. You return to a window similar to the window shown in Figure 100 on page 83.

Use the example shown in Figure 103 as a guide for the next three steps.

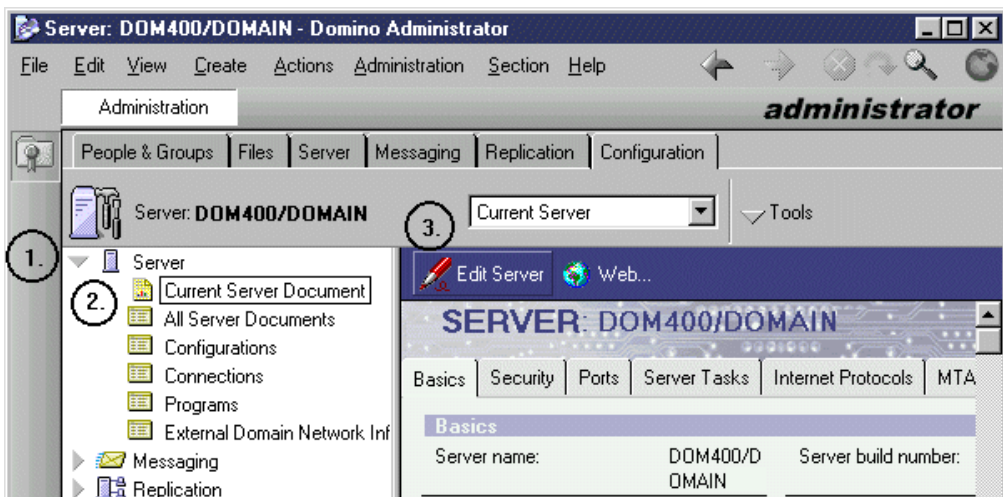


Figure 103. Server document

13. Open **Server** in the navigation tree (1).
14. Select **Current Server Document** (2).
15. Click the **Edit Server** button (3). The window shown in Figure 104 on page 85 appears.

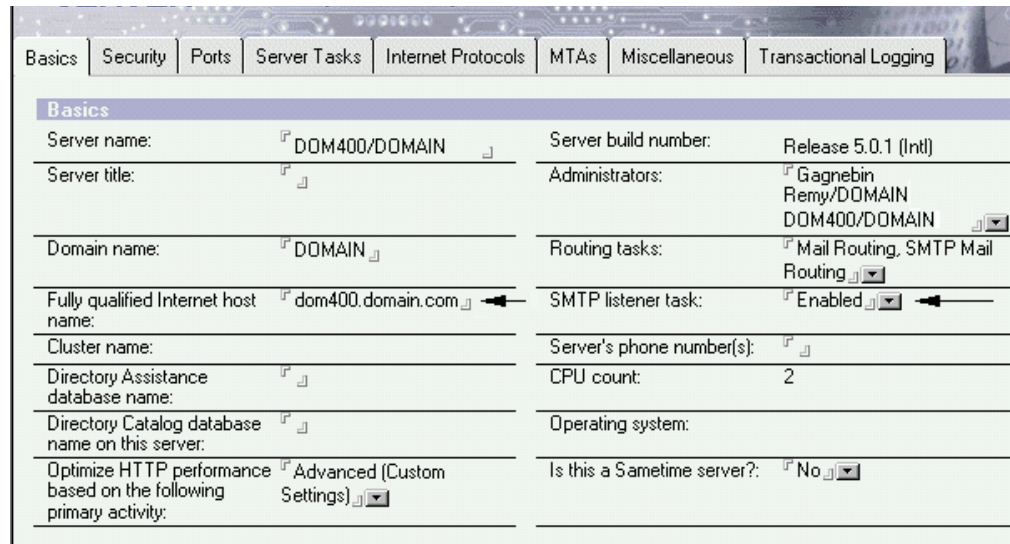


Figure 104. Server document - Basics

16. Verify that the Fully qualified Internet host name matches the Domino server name.
17. Verify that the SMTP listener task indicates *Enabled*.
18. Verify that the Routing tasks are *Mail Routing* and *SMTP Mail Routing*.
19. Click **Save and Close**.

You have now configured the Domino server to handle multiple SMTP domains.

3.7.8 Linking Domino server with the firewall

To link the Domino SMTP server with the firewall, perform the following steps. Use the example shown in Figure 105 as a guide for the first three steps.

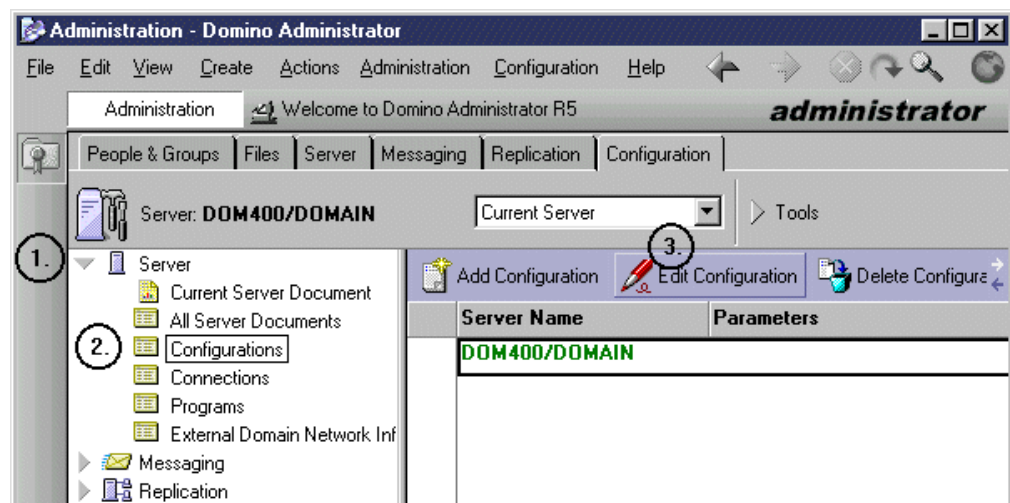


Figure 105. Configuration document

1. Open **Server** in the navigation tree (1).
2. Select **Configurations** (2).

3. Click the **Edit Configurations** button (3). The window shown in Figure 106 appears.

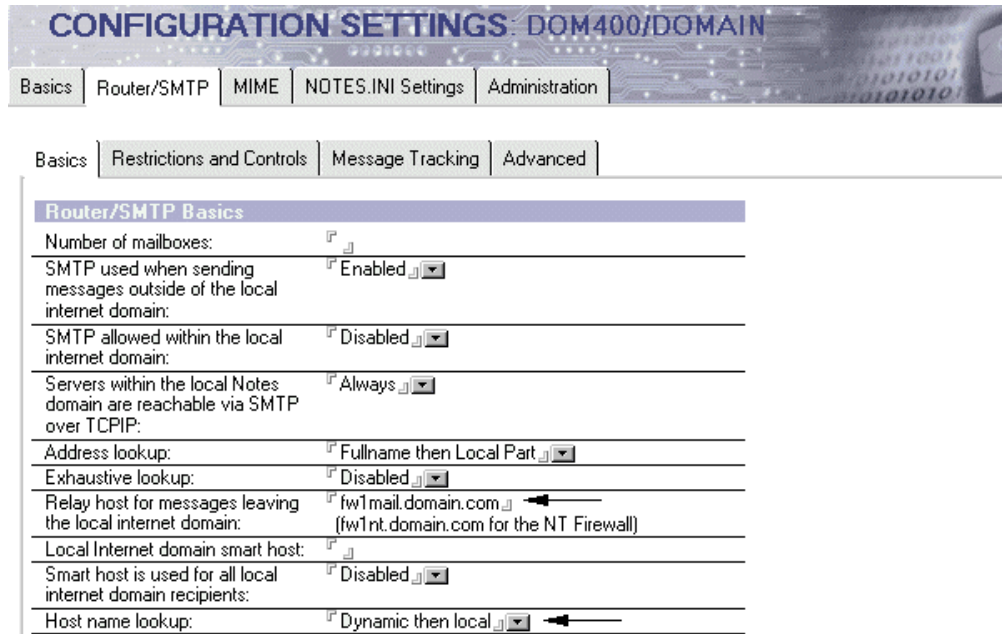


Figure 106. Configuration document - Router/SMTP

4. Click the **Router/SMTP** tab.
5. Enter the firewall name for Relay host for messages leaving the local Internet domain. Figure 106 shows the AS/400 firewall and the NT firewall name. In your configuration, you should only have one entry.
6. Verify that the Host name lookup is set to `Dynamic then local`.
7. Click **Save and Close**.

You successfully linked the Domino SMTP server with the SMTP relay function of your firewall.

3.7.9 Creating Lotus Notes mail users

The Domino server is now ready to receive mail from the Internet. In this section, we create a Lotus Domino user and their mailbox. To build the user and mailbox, perform the following steps. Use the example shown in Figure 107 on page 87 as a guide for the first five steps.

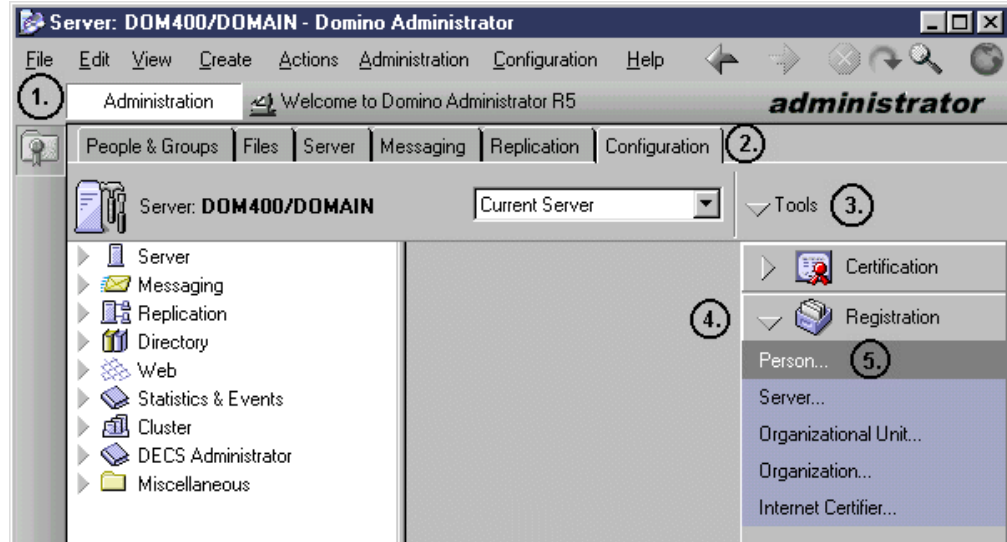


Figure 107. Registration - Person

1. On the Domino Administrator desktop, click **Administration** (1).
2. Click the **Configuration** tab (2).
3. Click the **Tools** pull-down menu (3).
4. Click **Registration** (4).
5. Click **Person** (5). The display shown in Figure 108 appears.



Figure 108. Certifier ID password

6. Enter the password, and click **OK**. The display shown in Figure 109 on page 88 appears.

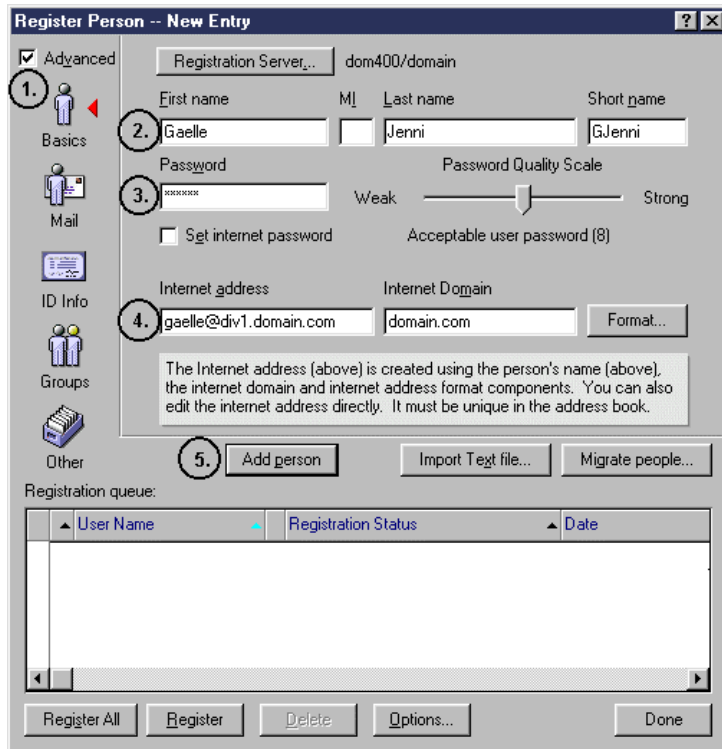


Figure 109. Register Person (Part 1 of 2)

7. Check **Advanced** (1).
8. Enter the person's first name and last name (2).
9. Enter the person's password (3).
10. Enter the person's Internet address and Internet domain (4).
11. Click the **Add person** button (5). The display shown in Figure 110 on page 89 appears.

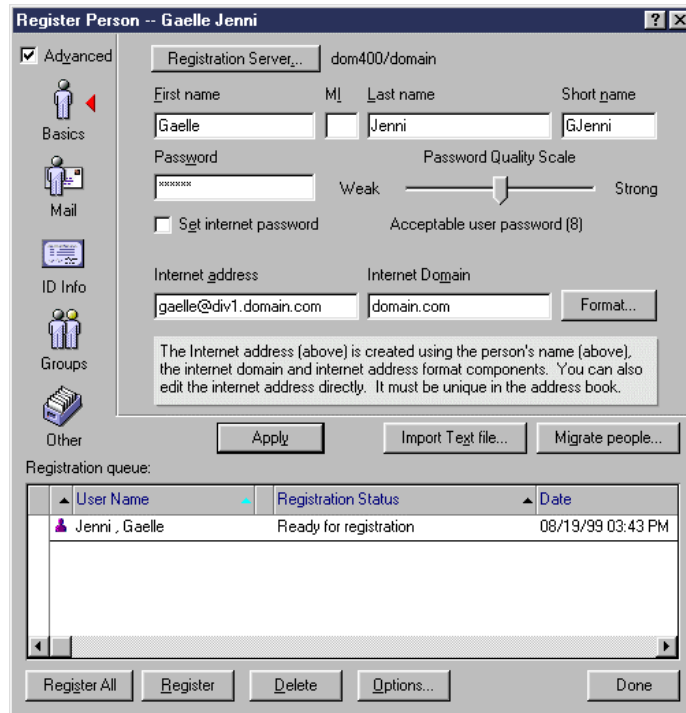


Figure 110. Register Person (Part 2 of 2)

12. Repeat steps 8 through 11 to add the next two users.

13. Click **Register All**.

The registration process can take several minutes.

You have now successfully registered your users and mailboxes. The user ID for each person is stored on the Domain's Public Address Book.

The last step is to configure Lotus Notes on your PCs. If you never before configured Lotus Notes for your mail, refer to the Lotus documentation that came with the product.

Chapter 4. Multiple domains on a single system

This chapter presents the procedures for configuring a firewall that supports a mail environment composed of multiple domains. All domains are processed by the same mail server. It also contains the procedures for setting up the configuration of both IBM Firewall for AS/400 and IBM eNetwork Firewall for Windows NT. Plus, you can find the procedures that we use to set up an SMTP and POP3 server or SMTP and Domino server on the AS/400 system.

4.1 Scenario

In this scenario, we present a corporation that has three companies, each with its own mail domain. The public mail domains and the private mail domains are the same.

The internal DNS can be on any AS/400 system on the network. In our scenario, the AS/400 HOME400 handles this function.

If you use the POP3 server, the SMTP server is on the AS/400 HOME400. If you use Domino server, the SMTP is managed by the Domino server DOM400. The firewall is either IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT

If you want to open the firewall to allow POP3 or Domino clients to access the internal mail server from the Internet, refer to 3.3.5, "Planning NAT to map the POP3 server address outside the firewall" on page 33, for IBM Firewall for AS/400. Refer to 3.4.5, "Planning NAT to map POP3 server address outside the firewall" on page 51, through 3.4.9, "Creating a service" on page 56, for IBM eNetwork Firewall for Windows NT.

4.1.1 Scenario network configuration

Figure 111 on page 92 illustrates a logical view of the network configuration used in this scenario. There are three ways to implement the firewall:

- The firewall is an Integrated Netfinity Server running IBM Firewall for AS/400.
- The firewall is a separate PC running Windows NT Server and IBM eNetwork Firewall for Windows NT.
- The firewall is an Integrated Netfinity Server running IBM eNetwork Firewall for Windows NT.

The procedure for setting up Windows NT Server on an Integrated Netfinity Server is provided in Chapter 8, "Installing a Windows NT Server to support firewalls" on page 289.

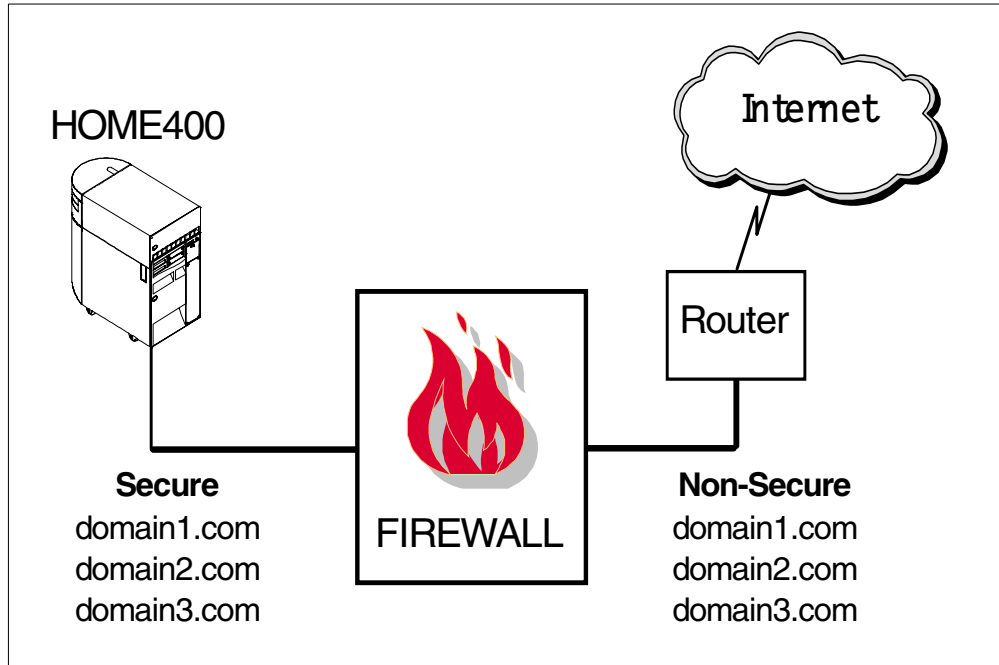


Figure 111. Scenario network configuration for multiple domains on a single server

4.1.2 Scenario objectives

The objectives of this scenario are:

- Configure the IP domains on the internal DNS.
- Configure the firewall so that it can handle the mail domains.
- Configure the POP3 server to handle internal and Internet mail.
- Configure the Domino server to handle internal and Internet mail.

4.1.3 Scenario advantages

This scenario has the following advantages:

- The firewall can be either IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT.
- IBM Firewall for AS/400 can handle the DNS function, so you do not need to spend extra money to handle this function by your ISP or on other DNS in the DMZ.
- Inbound mail is preceded in one single system. This is an opportunity to have an antivirus system scanning mail coming from the Internet.

4.1.4 Scenario limitations

There are also some limitations associated with this scenario. The DNS function of IBM eNetwork Firewall for Windows NT uses the NT DNS in a cache-only mode. This means that a DNS is needed in the DMZ or you will have to use the DNS of your ISP (using the ISP DNS may mean extra fees).

4.1.5 Planning considerations

Consider the following points when planning to implement:

- Is there any internal DNS in your company?
- Are the PCs configured to handle an internal DNS?
- Are you using AS/400 SMTP and POP or AS/400 Domino for mail?
- Are you using IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT as your firewall?

The remainder of this chapter documents the procedures used to set up the firewall and mail server using both firewall products and both mail products. You should choose the sections that are appropriate for your environment.

- FW2MAIL refers to IBM Firewall for AS/400.
- FW2NT refers to IBM eNetwork Firewall for Windows NT.
- HOME400 refers to the AS/400 system on the domain *domain.com*.
- DOM400 refers to the Domino server on AS/400 HOME400.

Table 10 lists the domain names, host names, and IP addresses used for this scenario.

Table 10. Domain names, host names, and IP addresses

Secure domain name	Host name	IP address
domain.com	fw2nt (non-secure)	208.222.150.250
domain.com	fw2nt	10.100.1.2
domain.com	fw2mail (non-secure)	208.222.150.250
domain.com	fw2mail	10.100.1.2
domain.com	fw2mail (internal LAN)	192.168.2.2
domain.com	home400	10.100.1.7
domain.com	home400 (internal LAN)	192.168.2.1
domain.com	dom400	10.100.1.8
(Host table entry)	domain1.com	10.100.1.3
(Host table entry)	domain2.com	10.100.1.4
(Host table entry)	domain3.com	10.100.1.5

Table 11 lists the values used to configure the AS/400 DNS for this scenario using different SMTP servers.

Table 11. Secure mail server name - DNS MX values

Firewall product	Secure and public domain name	MX value for mail server name for AS/400 SMTP	MX value for mail server name for Domino SMTP
IBM Firewall for AS/400	domain1.com	home400.domain.com.	dom400.domain.com.
	domain2.com	home400.domain.com.	dom400.domain.com.
	domain3.com	home400.domain.com.	dom400.domain.com.
IBM eNetwork Firewall for Windows NT	domain1.com	home400.domain.com.	dom400.domain.com.
	domain2.com	home400.domain.com.	dom400.domain.com.
	domain3.com	home400.domain.com.	dom400.domain.com.

Table 12 lists the values used to configure SMTP mail relay on the firewall for this scenario using the different firewall and mail products.

Table 12. Domain name and secure mail server name - Firewall values

Firewall product	Secure and public domain name	Firewall mail server name for AS/400 SMTP	Firewall mail server name for Domino SMTP
IBM Firewall for AS/400	domain1.com	domain1.com	domain1.com
	domain2.com	domain2.com	domain2.com
	domain3.com	domain3.com	domain3.com
IBM eNetwork Firewall for Windows NT	domain1.com	home400.domain.com	dom400.domain.com
	domain2.com	home400.domain.com	dom400.domain.com
	domain3.com	home400.domain.com	dom400.domain.com

In Table 13, list your domain names, host names, and IP addresses you need for this scenario.

Table 13. User values for domain name, host name, and IP address

Domain name	Host name	IP address

Domain name	Host name	IP address
(Host table entry)		
(Host table entry)		
(Host table entry)		

In Table 14, list the values you need to configure the AS/400 DNS for this scenario.

Table 14. User values for secure mail server name - DNS MX values

Firewall product	Secure domain name	MX value for mail server name for AS/400 SMTP	MX value for mail server name for Domino SMTP

In Table 15, list the values you need to configure the SMTP mail relay on the firewall for this scenario.

Table 15. User values for domain name and secure mail server name - Firewall

Firewall product	Secure and public domain name	Firewall mail server name for AS/400 SMTP	Firewall mail server name for Domino SMTP

4.1.6 Task summary

To set up this scenario, you must configure the DNS to support the mail environment (step 1), configure a firewall (step 2 or 3), and configure your mail server (steps 4 and 5, or step 6).

1. Configure the AS/400 DNS.
2. Configure IBM Firewall for AS/400.
3. Configure IBM eNetwork Firewall for Windows NT (FW2MAIL).
4. Configure the SMTP server on the AS/400 system (FW2NT).
5. Configure the POP3 mail on the AS/400 system.
6. Configure the Domino server for mail.

4.2 Configuring the AS/400 DNS

This section describes the tasks that you must perform to configure the internal AS/400 DNS to handle multiple domains on a single mail server. If the DNS is not already installed, refer to *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147.

4.2.1 Task summary

To configure the AS/400 DNS for this scenario, perform the following steps:

1. Configure the AS/400 DNS to handle the internal domain *domain.com*.
2. Add systems to *domain.com*
3. Add the three domains *domain1.com*, *domain2.com*, and *domain3.com*.
4. Configure the MX record for the domains.
5. Configure the internal DNS to forward the queries to the firewall.

4.2.2 Configuring the AS/400 DNS to handle the internal domain

To configure the AS/400 DNS, use Operations Navigator, which is included as part of Client Access Express for Windows.

To access the DNS configuration, select your **AS/400 system name** ->**Network**->**Server**->**TCP/IP**. Double click **DNS**. Click the + symbol beside the DNS Server - Home400 entry. The window shown in Figure 112 is displayed.

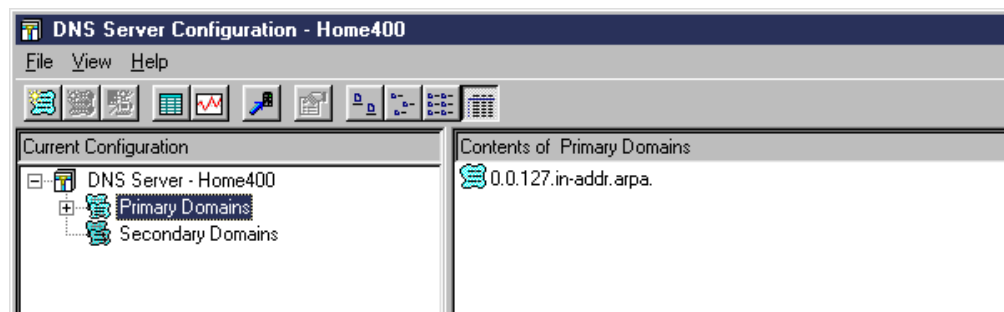


Figure 112. Configuring the AS/400 DNS to handle the internal domain: *domain.com*

To add the primary domain, perform the following procedure:

1. Right-click on **Primary Domains**. Select **New Primary Domain**. The window shown in Figure 113 on page 97 is displayed.

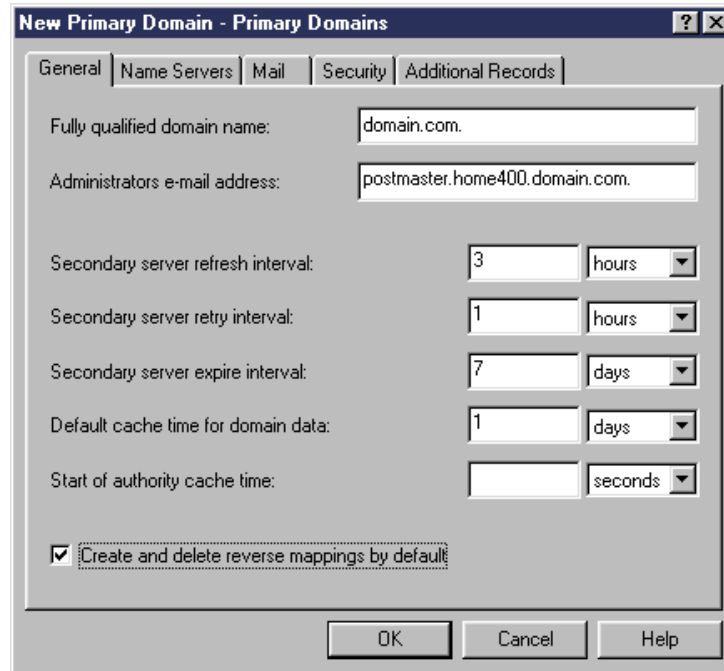


Figure 113. New Primary Domain domain.com

2. Enter the domain name `domain.com`. You *must* put a dot at the end of your domain since it is a fully qualified domain name.
3. Check **Create and delete reverse mappings by default**.
4. Click **OK**. The window shown in Figure 114 is displayed. Your domain name is displayed in the right-hand frame.
5. Right-click on the domain name you added. A drop-down menu appears. Click **Enable**. This enables the domain in the DNS.

You have now created the domain `domain.com`.

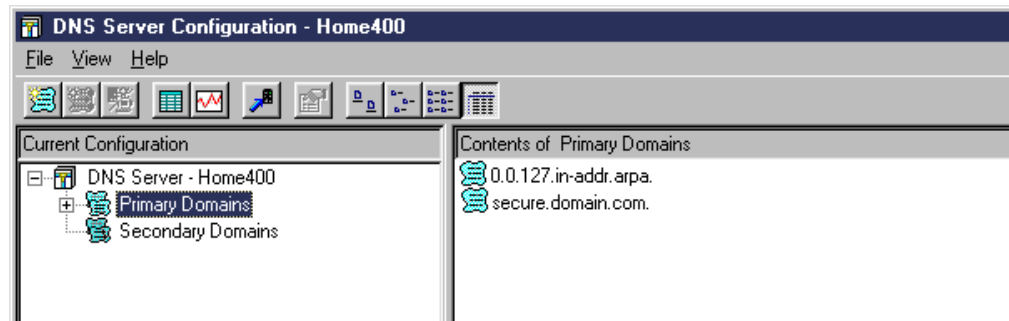


Figure 114. Content of Primary Domains after creating domain.com

4.2.3 Adding systems to the domain

After you create the domain, you need to add the mail server system, the Domino server (if you are using one), and the firewall name. To add the systems, perform the following steps:

1. Right-click **domain.com**.
2. Select **New Host**.
3. Click **Add**. The New Host window is displayed (Figure 115).

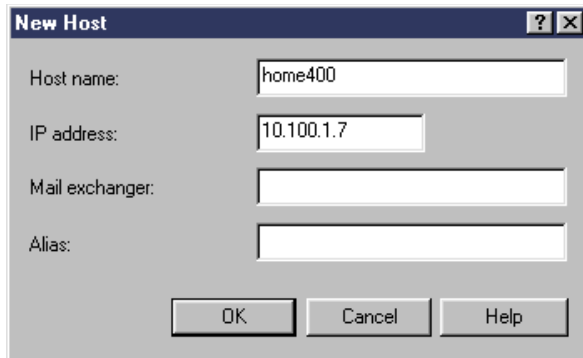


Figure 115. Adding the AS/400 host name

4. Enter the AS/400 host name and the IP address.
5. Click **OK**.

Repeat the steps in this section to add each host name needed for the domain. See Table 10 on page 93. Only the host names that have an IP address of 10.100.1.x need to be stored in the DNS.

Now that you added the system names to the DNS, you should continue setting up the DNS.

4.2.4 Adding the mail domains to the DNS

You now must add the three domains that you receive mail for to the DNS. In this scenario, the domain names are:

- domain1.com
- domain2.com
- domain3.com

To add the domains to the DNS, repeat the steps described in 4.2.2, “Configuring the AS/400 DNS to handle the internal domain” on page 96, for each domain name.

When you have completed adding all the domains, your DNS Server Configuration window should look similar to the one shown in Figure 116 on page 99. As a result of configuring our scenario, we have the following domains:

- 0.0.127.in-addr-arpa Reverse lookup for loopback domain 127.0.0
- 1.100.10.in-addr-arpa Reverse lookup for 10.100.1 domain
- domain.com Primary domain for systems
- domain1.com Mail domain for domain 1
- domain2.com Mail domain for domain 2
- domain3.com Mail domain for domain 3

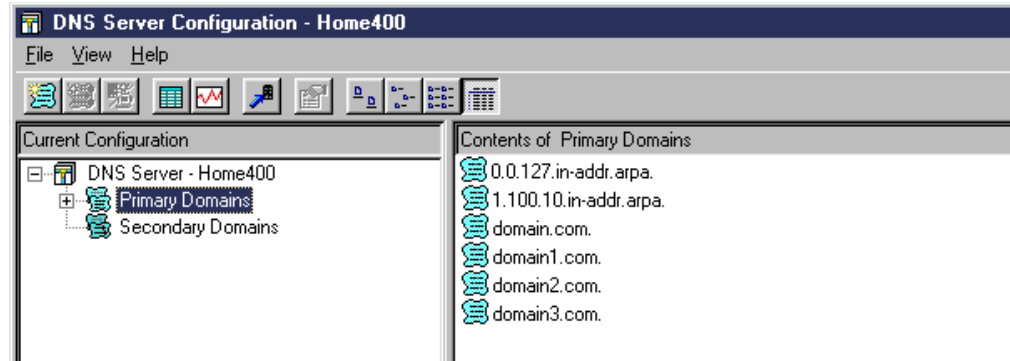


Figure 116. Content of Primary Domains after creating the three domains

If any of the domain names have a yellow exclamation mark (!) on them, they need to be enabled. Right-click on the domain name. A drop-down menu appears. Click **Enable**. This enables the domain in the DNS.

Now you need to add the mail exchange (MX) information for each of the mail domains.

4.2.5 Configuring the MX record for each of the three domains

The MX record tells the DNS client (it can be either a PC or another DNS) the name of the SMTP server that processes mail for the domain. Follow these steps to configure the MX for each of the three domains:

1. Right-click **domain1.com**.
2. Select **Properties**.
3. Click the **Mail** tab.
4. Click **Add**. The window shown in Figure 117 is displayed.

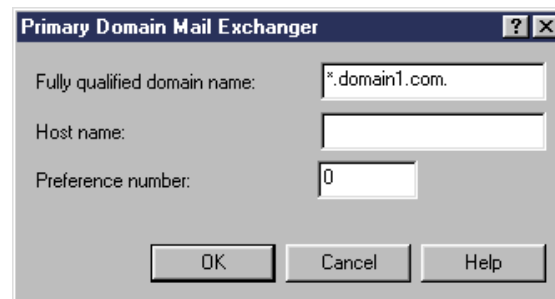


Figure 117. Adding an MX record in a domain

5. Remove the asterisk (*) from the front of the default domain name. In our example, we changed (*.domain1.com.) to domain1.com.
6. Enter the fully qualified host name of the SMTP server `home400.domain.com.` or `dom400.domain.com.` Refer to Table 11 on page 94 for the MX record value referred to the domain. Be sure to include the dot (.) at the end of the host name.
7. Click on **OK**.
8. Click on **OK** a second time to exit the Properties window.

Repeat the steps in this section to create an MX record for domains *domain2.com* and *domain3.com*.

4.2.6 Configuring the internal DNS to forward the queries to the firewall

The internal DNS cannot answer the queries that are intended to the Internet. It needs to be linked with the DNS firewall.

If an e-mail is sent to somebody@us.ibm.com, it first goes to the internal SMTP server. Then, it is forwarded to the firewall, and, from the firewall, it is sent to the Internet.

To set up DNS forwarding, you must change the DNS properties. You should start at the DNS Server Configuration window shown in Figure 118.

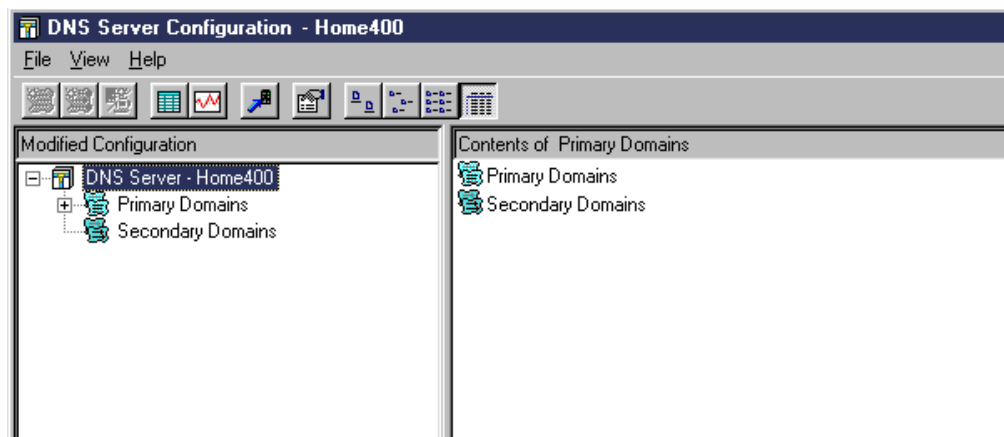


Figure 118. Configuring the internal DNS to forward queries to the firewall

Use the following procedure to change the properties of the DNS:

1. Right-click **DNS Server - Home400**.
2. Select **Properties**.
3. Click the **Forwarders** tab. The window shown in Figure 119 on page 101 is displayed.

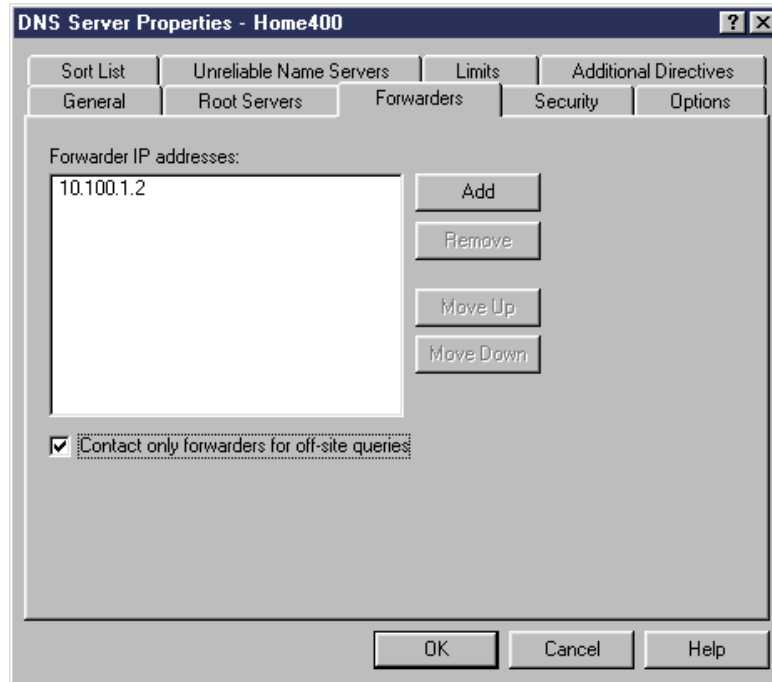


Figure 119. Adding the IP address of the firewall to the forwarders list

4. Click the **Add** button.
5. Enter the secure IP address of the firewall.
6. Check **Contact only forwarders for off-site queries**.
7. Click **OK**.

The DNS configuration is now ready to handle your SMTP mail. Stop and start the DNS server, or click **File->Update Server** to update the DNS server configuration and make your configuration available.

4.3 Configuring IBM Firewall for AS/400 (FW2MAIL)

This section describes the tasks that you must perform to configure IBM Firewall for AS/400 to handle multiple domains on a single mail server.

4.3.1 Scenario network configuration

Figure 120 on page 102 shows the network configuration used in this scenario. In this portion of the scenario, we use an Integrated Netfinity Server to run IBM Firewall for AS/400. The network diagram is the same if we use IBM eNetwork Firewall for Windows NT. The *Internal LAN and one LAN adapter make up the secure side of the network. The other LAN adapter is used to connect to the ISP router.

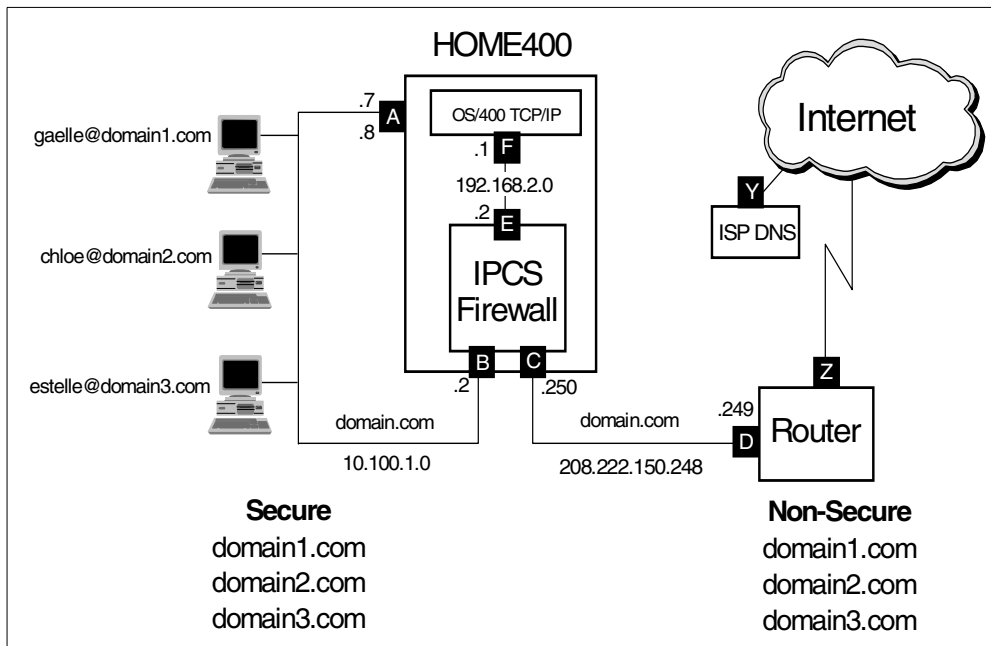


Figure 120. Multiple domains on a single mail server with IBM Firewall for AS/400

4.3.2 Task summary

The following list summarizes the tasks used to configure IBM Firewall for AS/400:

1. Install IBM Firewall for AS/400.
2. Perform the basic configuration.
3. Remove the MX record for domain *domain.com*.

4.3.3 Installing IBM Firewall for AS/400 (FW2MAIL)

Install the firewall at the local site using the instructions in the manual *Getting Started with IBM Firewall for AS/400*, SC41-5424. A summary of the installation parameters is shown on the Complete the Firewall Installation summary page in Figure 121 on page 103.



Complete the Firewall Installation

Review the information that you have entered. Make any changes on this page. When you are sure that the information is correct, click the **Install** button to complete the firewall installation. This step takes several minutes to run. Please be patient.

Firewall Name	FW2MAIL		
Firewall Resource Name	CC02		
Router IP Address	208	222	150 . 249
Route Destination	Subnet Mask		Next Hop
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	Port 1	Port 2	
LAN Type	Token Ring (16Mb)	Token Ring (16Mb)	
Adapter Address	400000000037	400000000250	
IP Address	10 . 100 . 1 . 2	208 . 222 . 150 . 250	
Subnet Mask	255 . 255 . 255 . 0	255 . 255 . 255 . 248	

Figure 121. Firewall Installation summary page (FW2MAIL)

Start the firewall by clicking **Start** (Figure 122).



Start the Firewall

The firewall takes several minutes to start. Please be patient. Click **Start** to start the firewall.

Figure 122. Starting the firewall (FW2MAIL)

4.3.4 Performing basic configuration (FW2MAIL)

Perform the basic configuration of the local firewall. For further information, refer to *Getting Started with IBM Firewall for AS/400*, SC41-5424, and the redbook *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162.

In the Review Configuration, be aware that the *Secure Mail Server* and the *Secure Domain* refer to the internal mail domain name. The SMTP domain name in the inbound e-mail (the value to the right of the @ symbol) is changed to the value in the *Secure Mail Server* column. This value must match the SMTP mail

address setup for the user on the secure mail server. In our scenario, these values have to be exactly the same, because of the domain names selected for our internal users. The value in the Secure Mail Server parameter is used in an MX record DNS query to find the SMTP server that processes the mail. If the query fails, an A record DNS query is done for the value. If an IP address is returned, the mail is routed to the mail server. In most cases, it is easiest to use the same value for the Secure Mail Server and the Secure Domain parameters and let the internal DNS MX records point to the secure mail server system. Refer to Table 12 on page 94 for information about the domain name and secure mail server name.

If you do not have a DNS server in the secure network, this technique will not work. You must specify the fully qualified name of the secure mail server (for example, `hostname.domain.com`) in the Secure Mail Server column. This means that the e-mail address of the users will be in the form `userid@hostname.domain.com`.

In this configuration, we create all four domains during the basic configuration. This is the easiest way to create a domain in IBM Firewall for AS/400. This means that, in this scenario, *domain.com* is visible on the Internet.

We recommend that you link the firewall DNS with multiple DNS servers in the outside world. If one fails, you can still continue to send e-mail and surf the Web. In our scenario, the three DNS servers belong to the ISP.

For more information about IBM Firewall for AS/400, refer to Appendix D, "Firewall concepts" on page 349.

Figure 123 on page 105 and Figure 124 on page 106 show the Review Configuration for FW2MAIL (refer to Figure 120 on page 102 for the scenario network configuration).



Review Configuration

Review the information that you have entered. Make any changes on this page. When you are sure that the information is correct, print the page for future reference. This creates all the firewall configuration settings. This may take a few minutes to run, so please be patient.

Your AS/400 is: HOME400.DOMAIN.COM

Your firewall is: FW2MAIL

Secure domain name servers:

10.100.1.7

Secure Port	IP Address	Subnet Mask
<input checked="" type="radio"/> Port 1	10.100.1.2	255.255.255.0
<input type="radio"/> Port 2	208.222.150.250	255.255.255.248

Secure Mail Server	Secure Domain	Public Domain
domain.com	domain.com	domain.com
domain1.com	domain1.com	domain1.com
domain2.com	domain2.com	domain2.com
domain3.com	domain3.com	domain3.com

Name Server	IP Address
dns1.isp.com	194.41.0.4
dns2.isp.com	128.9.0.107
dns3.isp.com	192.33.4.12

Figure 123. Basic firewall configuration summary page for FW2MAIL (Part 1 of 2)

Public Server	Public IP Address	Private IP Address

Services	Proxy	SOCKS	NAT
HTTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HTTPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FTP (passive)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FTP (active)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Telnet	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Secure Telnet		<input type="checkbox"/>	<input type="checkbox"/>
Gopher	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WAIS			<input type="checkbox"/>
IRC		<input type="checkbox"/>	<input type="checkbox"/>
RealAudio			<input type="checkbox"/>
Lotus Notes		<input type="checkbox"/>	<input type="checkbox"/>
LDAP		<input type="checkbox"/>	<input type="checkbox"/>
Secure LDAP		<input type="checkbox"/>	<input type="checkbox"/>
Server Mapper		<input type="checkbox"/>	<input type="checkbox"/>
DRDA		<input type="checkbox"/>	<input type="checkbox"/>
POP3 Mail		<input type="checkbox"/>	<input type="checkbox"/>
NNTP		<input type="checkbox"/>	<input type="checkbox"/>
Secure NNTP		<input type="checkbox"/>	<input type="checkbox"/>

If you selected any NAT services, then specify the translation of private to public IP addresses.

NAT	IP Address	Mask
Private	10.100.1.2	255.255.255.0
Public		

OK Cancel

Figure 124. Basic firewall configuration summary page for FW2MAIL (Part 2 of 2)

The firewall is now ready for you to perform the basic configuration. Complete the following steps:

1. Click **OK**. A confirmation page is shown, which indicates that the firewall is configured (Figure 125).



You have successfully configured the firewall. The next step is to restart the firewall servers so that your configuration changes take effect. This will only take a short time. Do you want to restart the firewall?

Figure 125. Confirmation that the firewall is configured

2. Click **Yes**.

4.3.5 Removing MX record for the domain *domain.com*

During the basic configuration, we set up the domain *domain.com*. This domain does not handle mail. Because we defined it during basic configuration, the firewall has automatically created an MX record (mail exchanger) for this domain. If the domain was not listed as a mail domain during basic configuration, we would not have to remove it. We included it so we could show how to remove it now. To remove the domain for mail, perform the following steps:

1. To begin, click **Mail** on the Configuration Menu page (Figure 126).



Basic Create the basic firewall settings. This is a good place to start if this is the first time you have configured a firewall.

The following items are for experienced firewall administrators:

Basic Fastpath Create the basic firewall settings.

Logging Change the logging settings.

Notification Change the notification settings.

Filters Change the IP packet filter settings.

Proxy Change the proxy server settings.

SOCKS Change the SOCKS server settings.

DNS Change the domain name server settings.

Mail Change the mail settings.

Port Change the secure port.

Autostart Change the autostart settings.

VPN Change the VPN (Virtual Private Network) settings.

NAT Change the NAT (Network Address Translation) settings.

Figure 126. Mail selection in the Configuration Menu

The Secure Mail Servers page is displayed as shown in Figure 127.

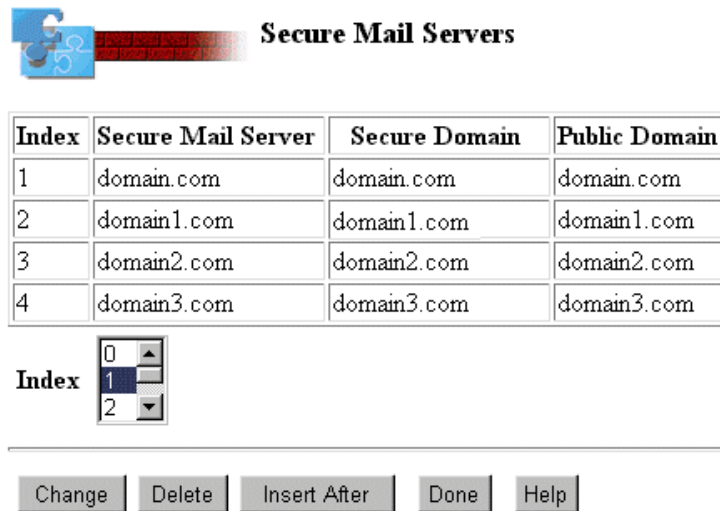


Figure 127. Secure Mail Servers window

2. Select the entry to be deleted.
3. Click **Delete**.
4. Click **OK**.

You must now restart the DNS and Mail Services of the firewall.

5. Click the **Administration** icon, and then click **Status** from the Administration Menu page. Select **Restart** for DNS and Mail as shown in Figure 128.



Figure 128. Restarting DNS and Mail from the Status window

6. Click **OK**.
7. Click **Done**.

IBM Firewall for AS/400 configuration is now ready. For more information about IBM Firewall for AS/400, refer to Appendix D, "Firewall concepts" on page 349.

4.4 Configuring IBM eNetwork Firewall for Windows NT (FW2NT)

This section describes the tasks that you must perform to configure IBM eNetwork Firewall for Windows NT to handle multiple domains on a single mail server.

4.4.1 Scenario network configuration

The network configuration for this scenario is shown in Figure 129.

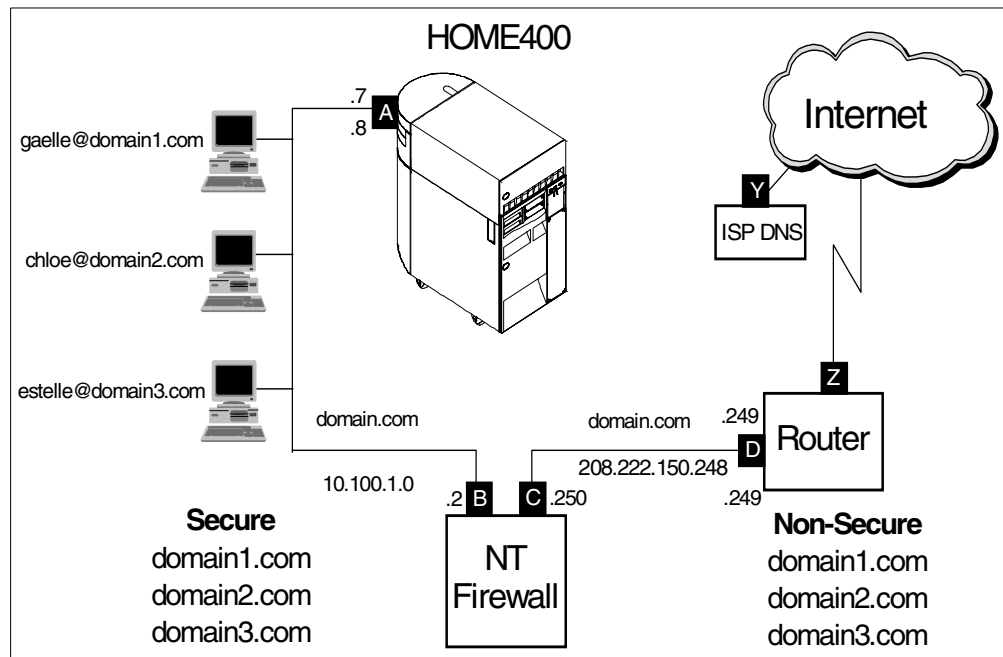


Figure 129. Multiple domains on a single mail server - NT

4.4.2 Task summary

The following list summarizes the tasks used to configure IBM eNetwork Firewall for Windows NT:

1. Install IBM eNetwork Firewall for Windows NT.
2. Set up IBM eNetwork Firewall for Windows NT.

4.4.3 Installing IBM eNetwork Firewall for Windows NT (FW2NT)

Install the firewall on the Windows NT PC using the instructions in *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT*, SG24-5209.

If you do not have this rebook and do not have Internet access to download it, complete the following steps:

1. Install the Windows NT server operating system.
2. Install the DNS Server for the Windows NT server.
3. Install the latest Service Pack for Windows NT server. Service Pack 4 is the minimum level required. Do not install IBM eNetwork Firewall for Windows NT on the system without the Service Pack.
4. Create a local user with Administrator authority.
5. Install the IBM NDIS intermediate driver.
6. Activate IP forwarding in the TCP/IP parameters.
7. Install the firewall product.

4.4.4 Setting up IBM eNetwork Firewall for Windows NT

Follow these steps to set up IBM eNetwork Firewall for Windows NT:

1. Run the **Configuration Client** in the IBM Firewall folder.
2. Log in with a user that has administrator authority.
3. To start basic configuration, click **Setup Wizard** in the **Help** menu (Figure 130).

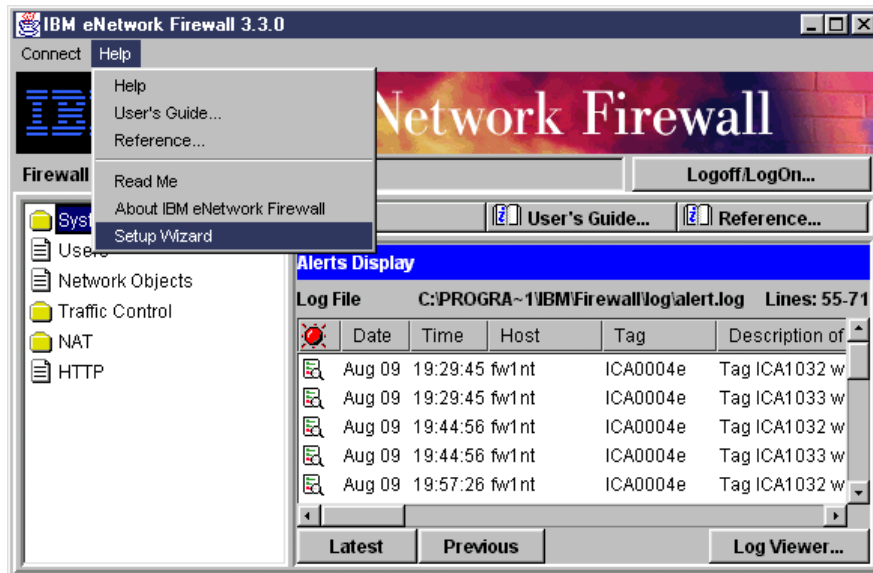


Figure 130. Starting firewall wizard

The Welcome window appears (Figure 131 on page 111). Read the window carefully.

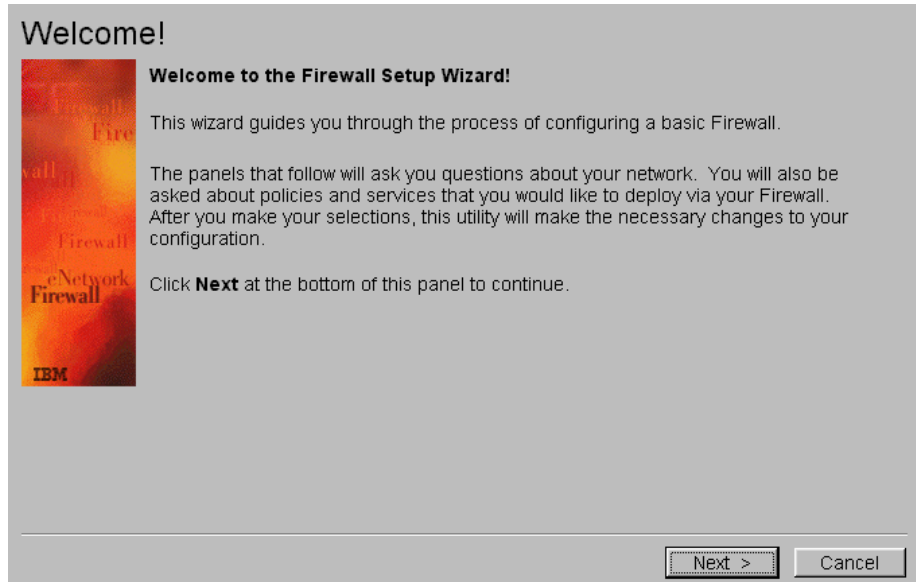


Figure 131. Welcome screen firewall wizard

Click **Next**. The window shown in Figure 132 appears. Read the window carefully.

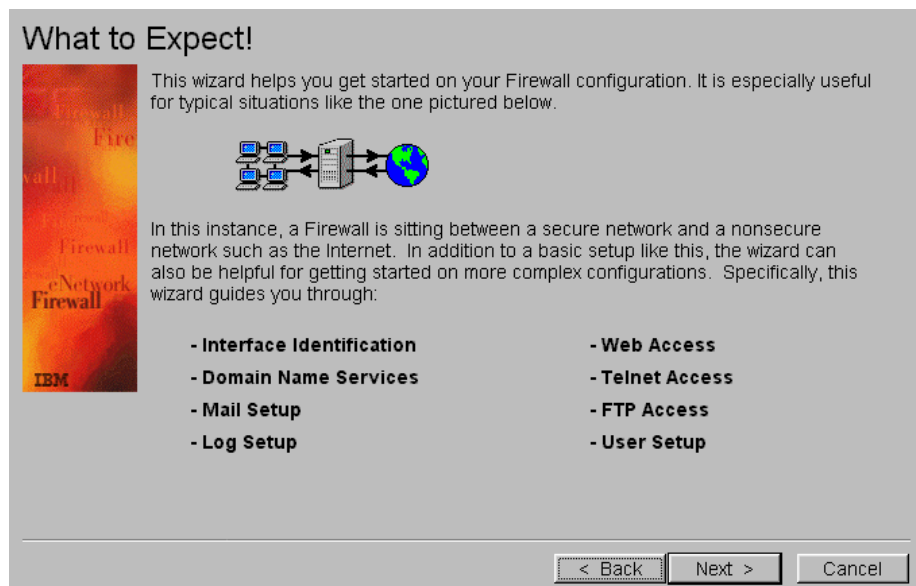


Figure 132. What to Expect firewall wizard

4. Click **Next**. The window shown in Figure 133 on page 112 appears. Read the window carefully.



Figure 133. Important notice firewall wizard

5. Click **Next**. The window shown in Figure 134 appears. Choose the secure interface.

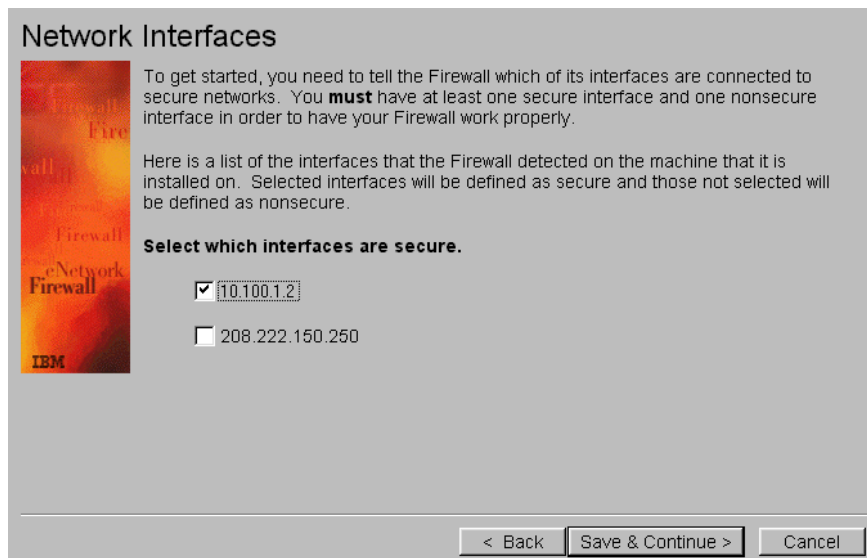


Figure 134. Network interface selection

6. Click **Save & Continue**. The window shown in Figure 135 on page 113 appears.

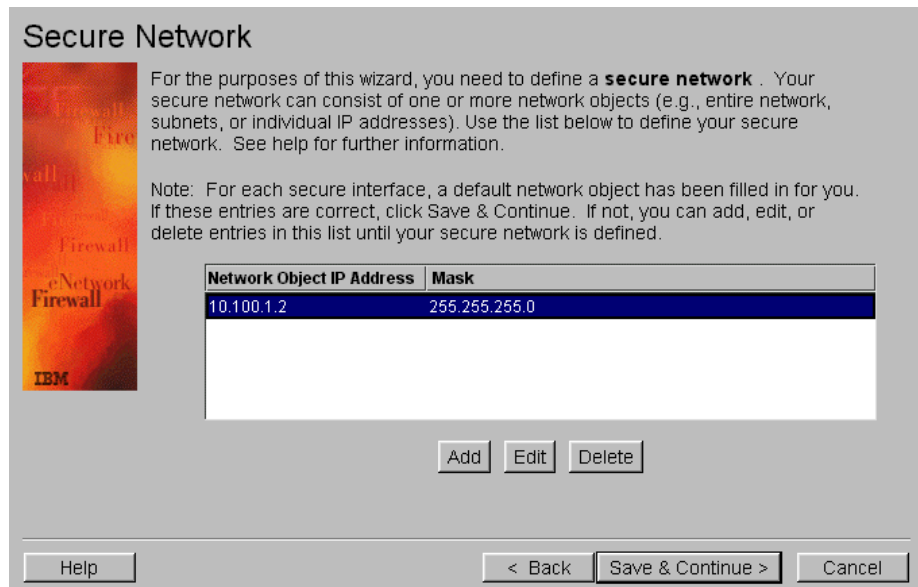


Figure 135. Secure Network configuration

7. Define your secure network. In the window shown in Figure 135, the wizard is guessing that your secure network is any IP address that starts with 10.100.1.
8. Click **Save & Continue**. The window shown in Figure 136 appears.

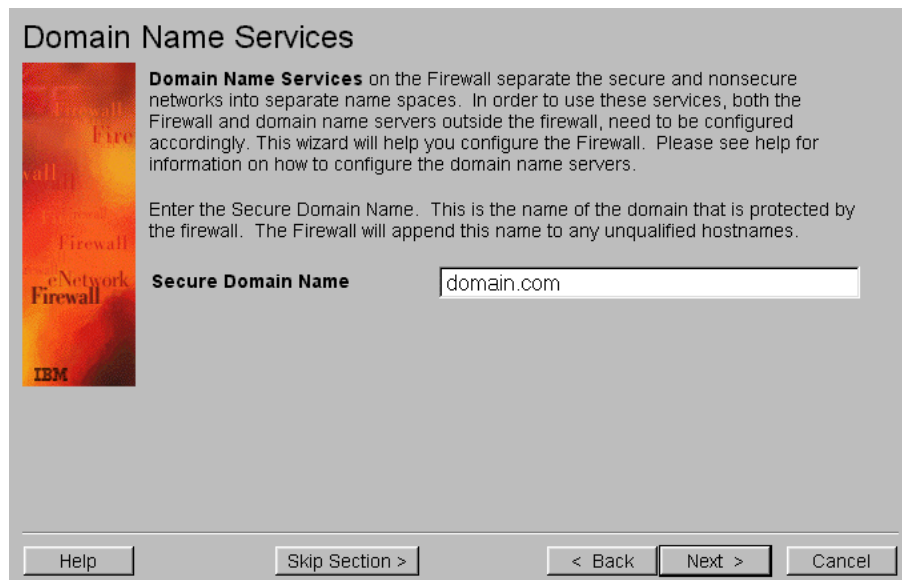


Figure 136. Domain Name Services

9. Enter the name of your internal domain name. This domain is protected by your firewall.
10. Click **Next**. The window shown in Figure 137 on page 114 appears.

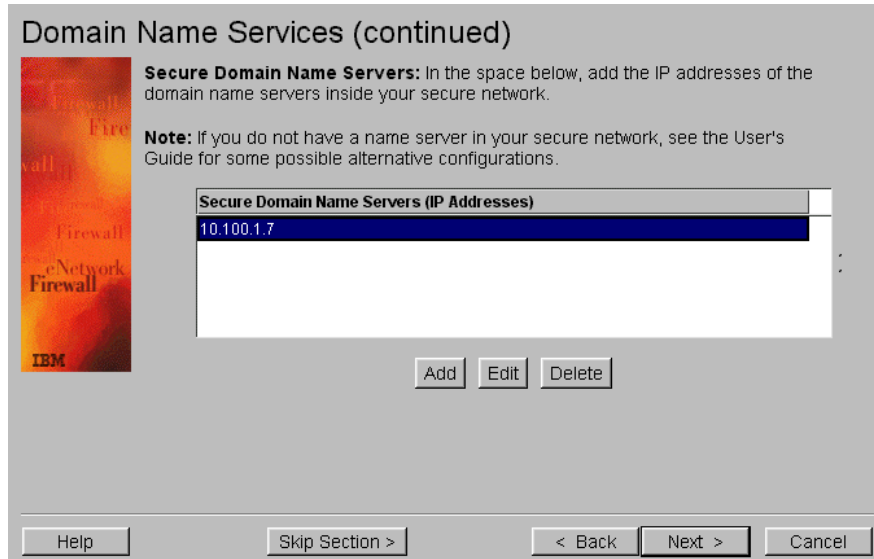


Figure 137. Secure DNS IP address

11. Enter the IP address of the secure internal DNS.

12. Click **Next**. The window shown in Figure 138 appears.

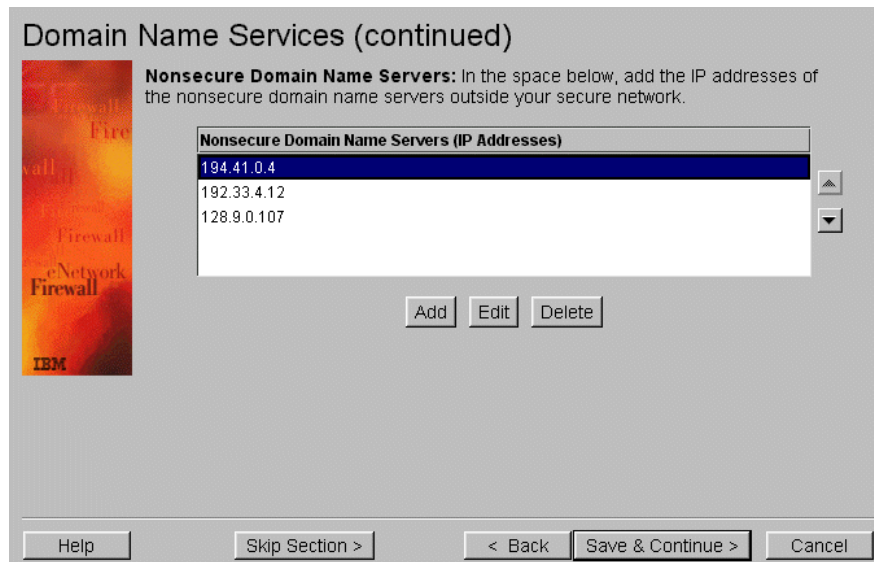


Figure 138. Non-secure DNS IP addresses

13. Click **Add**.

14. Enter the IP address of the non-secure DNS (ISP DNS).

15. Click **Next**.

16. Repeat steps 13 through 15 if the firewall DNS is linked with more DNS (recommended).

17. Click **Save & Continue**. The window shown in Figure 139 on page 115 appears.

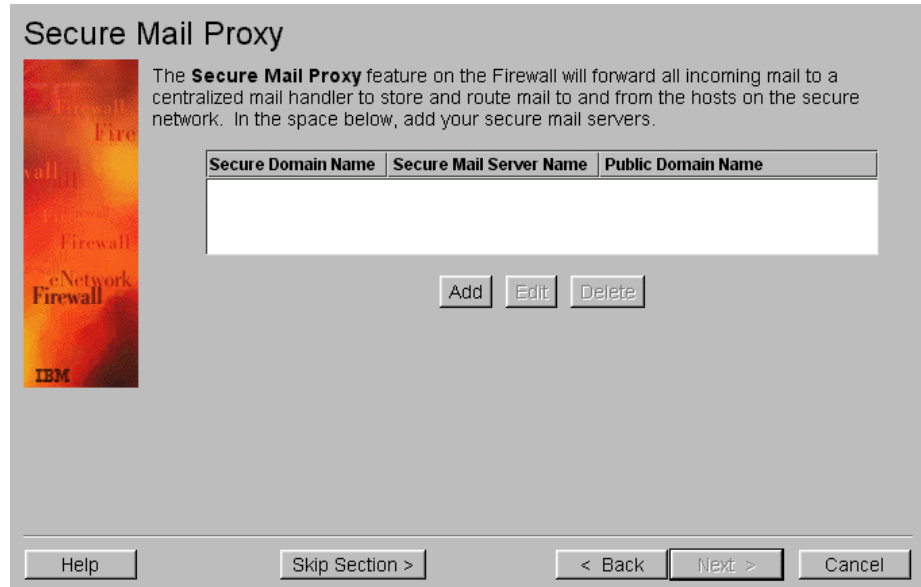


Figure 139. Secure Mail Proxy

18. Click **Add**. The window shown in Figure 140 appears.

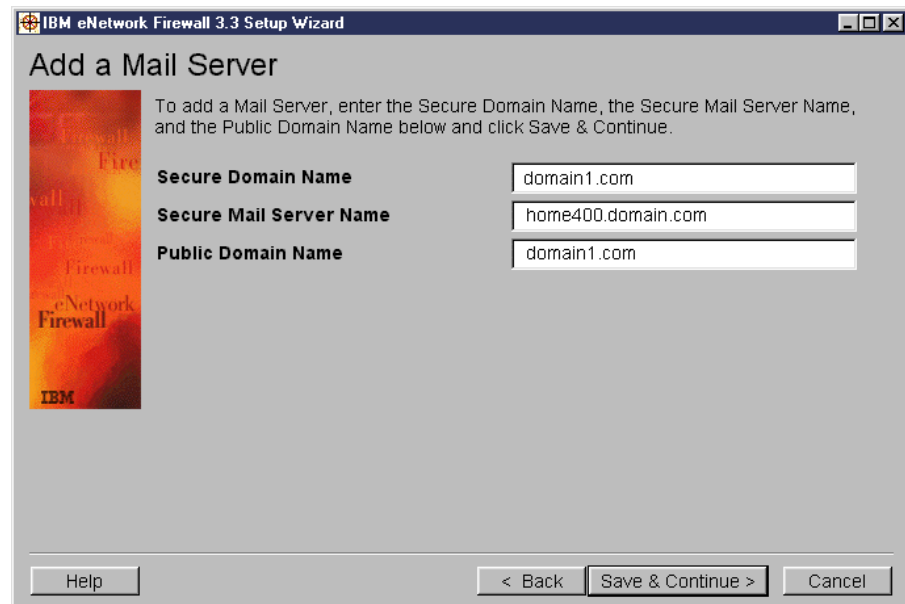


Figure 140. Adding a secure mail server

19. Enter your Secure Domain Name, Secure Mail Server Name, and Public Domain Name. Refer to Table 12 on page 94 for information about domain names and secure mail server names. Click **Save & Continue**. The window shown in Figure 141 on page 116 appears.



Figure 141. Secure Mail Proxy

20.Repeat steps 18 and 19 for *domain2.com* and *domain3.com*.

21.Click **Next**. The window shown in Figure 142 appears.

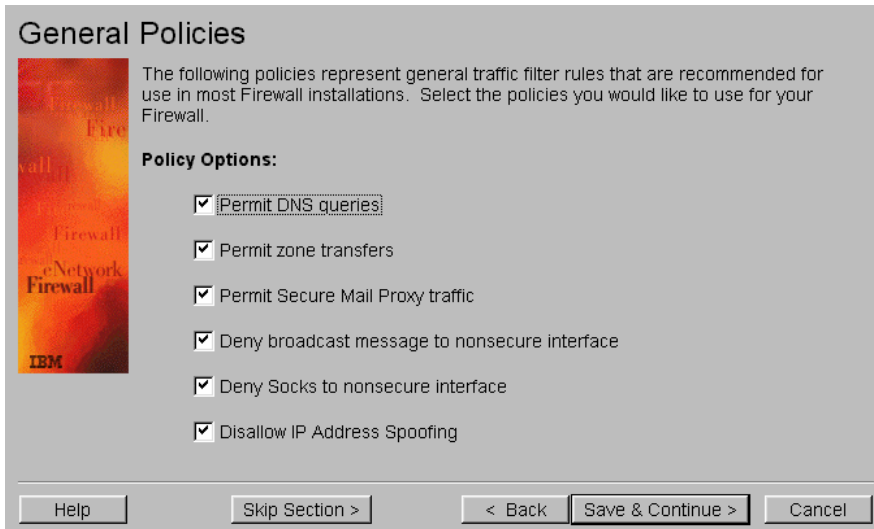


Figure 142. Security policies configuration

22.The marked options that you see under Policy Options are recommended for most firewall installations. Click **Save & Continue**. The window shown in Figure 143 on page 117 appears.

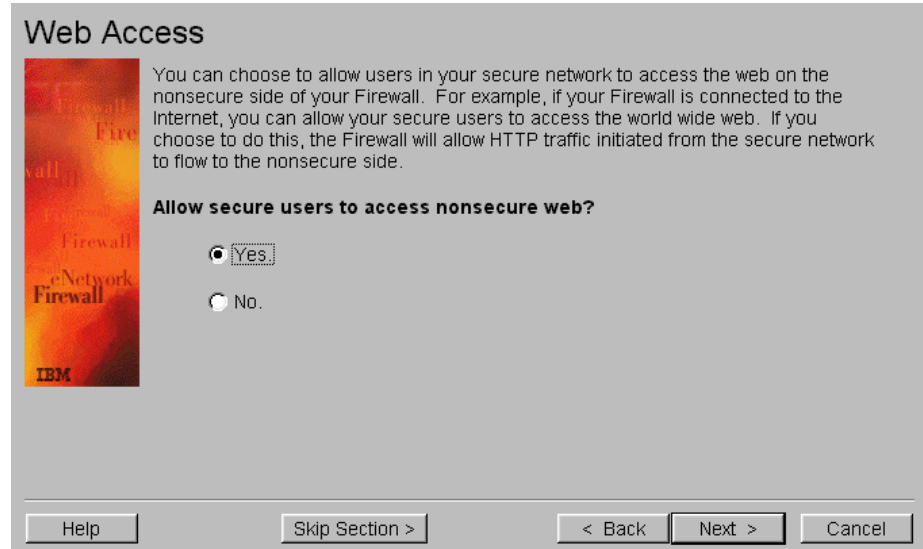


Figure 143. Web Access

23. Specify whether to allow Internet access to users. Click **Next**. The window shown in Figure 144 appears.

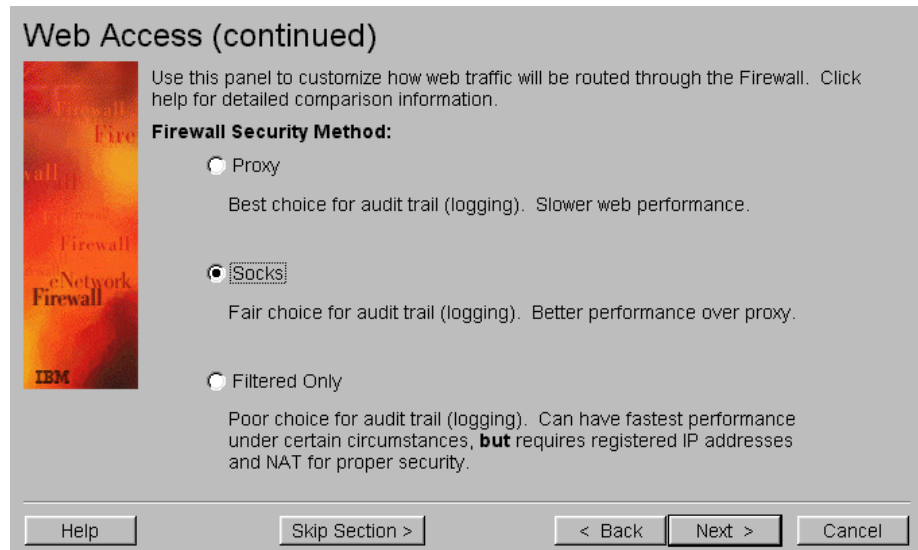


Figure 144. Web Access via Proxy, Socks, or Filtered Only

24. Define which Web access matches the best with your company. Click **Next**. The window shown in Figure 145 on page 118 appears.



Figure 145. Web Access services

25. Select which services are allowed. Click **Save & Continue**. The window shown in Figure 146 appears.

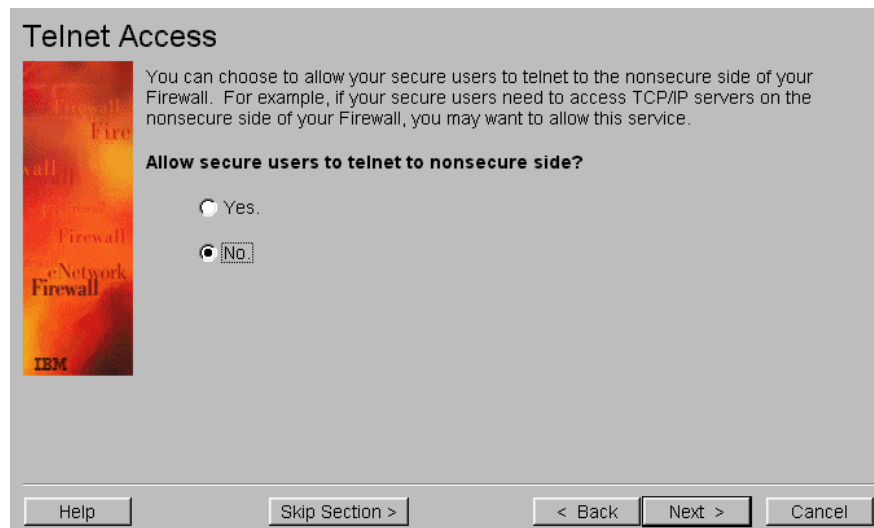


Figure 146. Telnet Access

26. Specify whether to allow Telnet access on the non-secure port of the firewall. Click **Next**. The window shown in Figure 147 on page 119 appears.

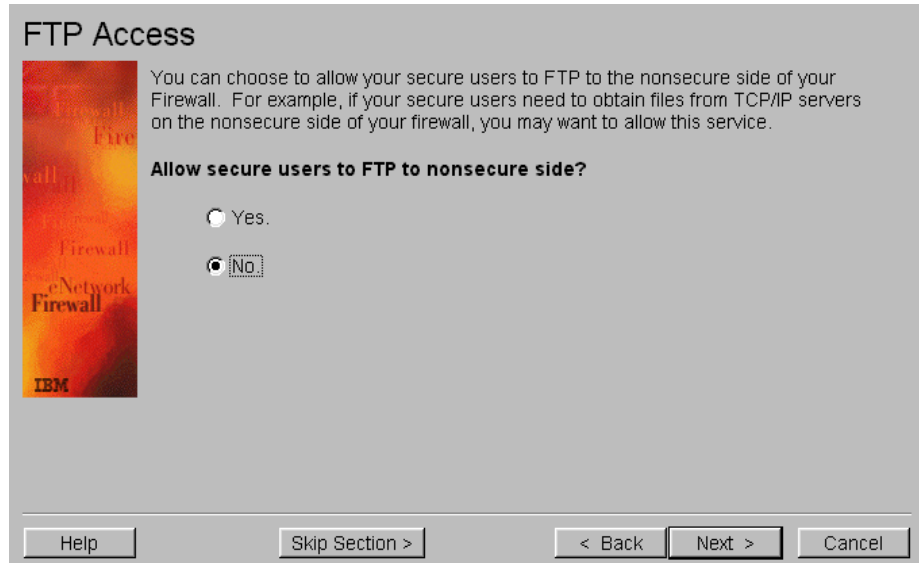


Figure 147. FTP Access

27. Specify whether to allow FTP access on the non-secure port of the firewall. Click **Next**. The window shown in Figure 148 appears.

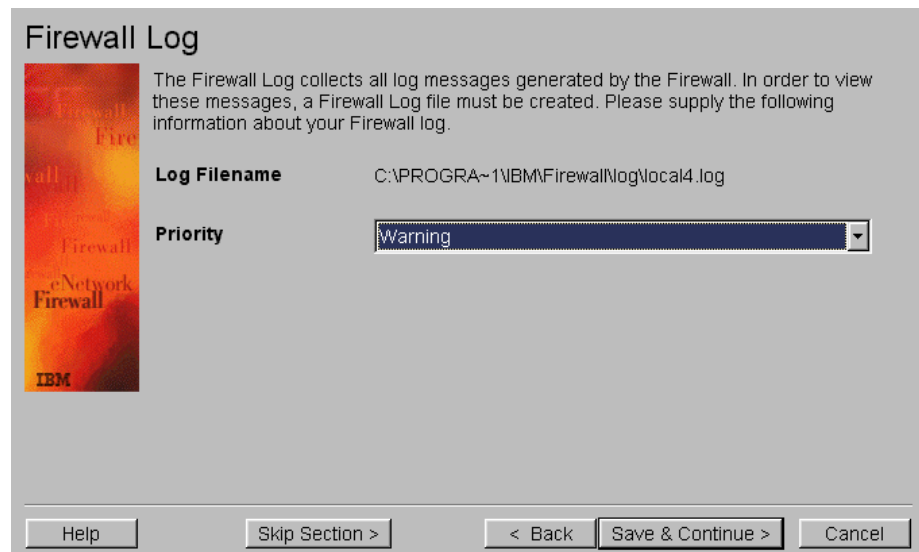


Figure 148. Firewall Log

28. Choose which level of logs are stored on the firewall database. Click **Save & Continue**. The window shown in Figure 149 on page 120 appears.

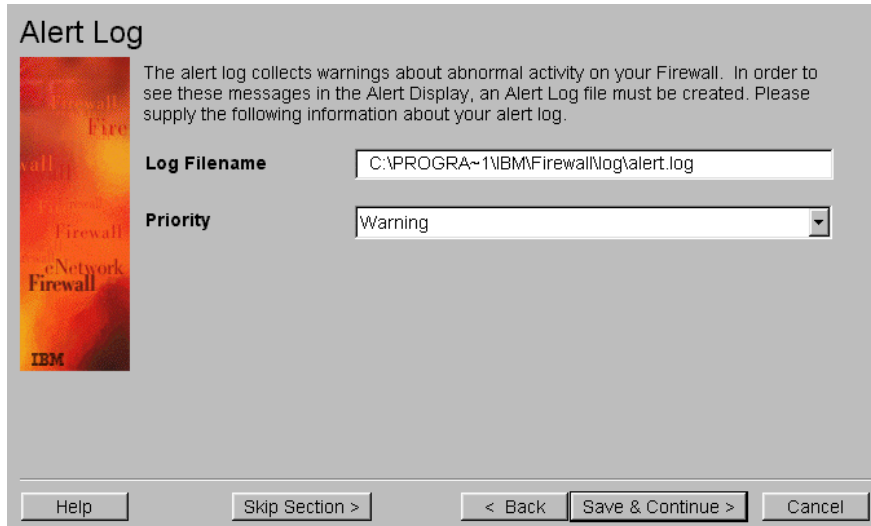


Figure 149. Alert Log

29. Choose which level of logs are stored on the alert database. Click **Save & Continue**. The window shown in Figure 150 appears.

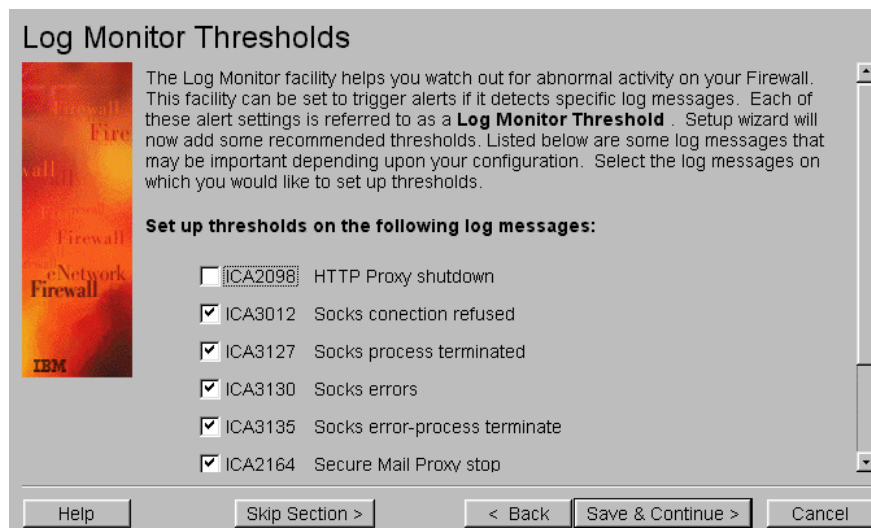


Figure 150. Log Monitor Thresholds

30. Select the thresholds. Click **Save & Continue**. The window shown in Figure 151 on page 121 appears.

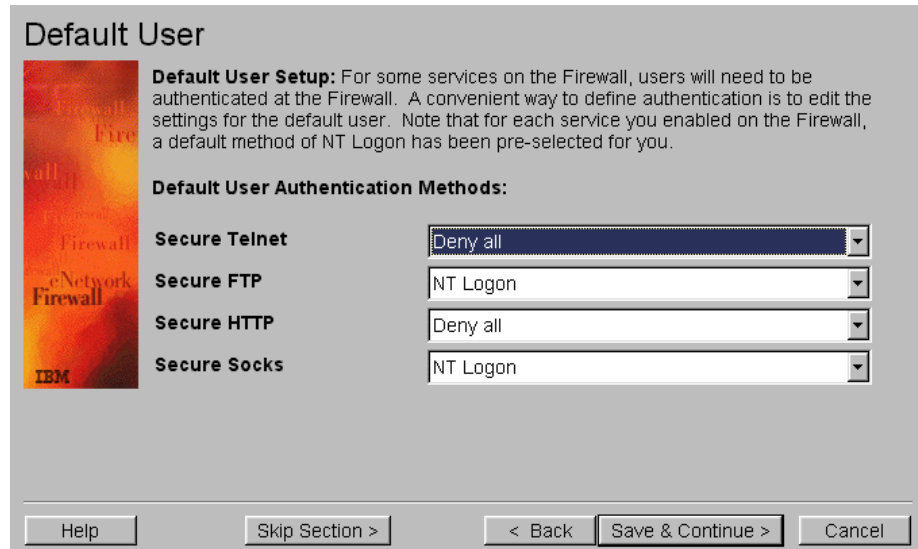


Figure 151. Default User setup

31. For some services, a firewall user needs to be authenticated. Click **Save & Continue**. The window shown in Figure 152 appears.

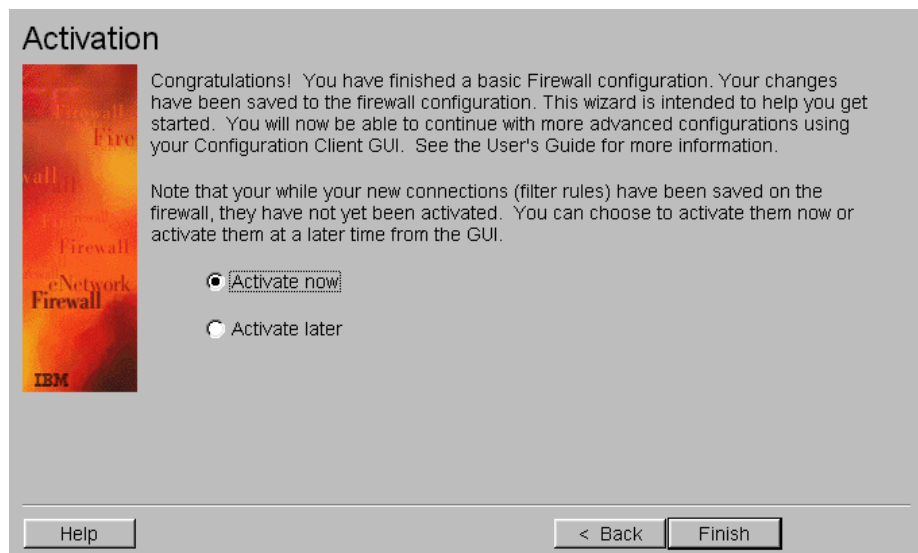


Figure 152. Setup Activation

32. You can choose to activate your configuration now or at a later time. Click **Finish**.

IBM eNetwork Firewall for Windows NT configuration is now ready. For more information about IBM eNetwork Firewall for Windows NT, refer to Appendix D, “Firewall concepts” on page 349.

4.5 Configuring the SMTP server on the AS/400 system

This section describes the tasks that you must perform to install and configure an SMTP server to handle multiple domains using a firewall.

4.5.1 Task summary

The following list summarizes the tasks used to implement the SMTP server on the AS/400 HOME400:

1. Set up the SMTP attributes.
2. Verify the HOME400 TCP/IP domain name information.
3. Handle multiple SMTP domains on a single AS/400 system.
4. Add the firewall name to the host table entries.
5. Start the SMTP server.

4.5.2 Setting up SMTP attributes

To route mail for Internet users to the firewall, you *must* configure the SMTP attributes in the AS/400 system to point to the firewall as the mail router. Entering the firewall name in the Mail router field tells the SMTP server where to forward mail that it cannot deliver itself. Complete the following steps:

1. On an AS/400 command line, type:

```
CHGSMTPA
```
2. Press **F4**, and then press Page Down.
3. You *must* enter ***YES** in the Firewall field. This tells the SMTP server that it is located behind a firewall.
4. Enter the correct values as shown in Figure 153, and press Enter.

```
Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

User ID delimiter . . . . . '?'          *SAME, *DFT, ?, =, ., &, $...
Mail router . . . . . > fw2mail.domain.com
                               (fw2nt.domain.com for the NT firewall)

Coded character set identifier    00819      1-65533, *SAME, *DFT
Mapping tables:
  Outgoing EBCDIC/ASCII table .  *CCSID   Name, *SAME, *CCSID, *DFT
  Library . . . . .                Name, *LIBL, *CURLIB

  Incoming ASCII/EBCDIC table .  *CCSID   Name, *SAME, *CCSID, *DFT
  Library . . . . .                Name, *LIBL, *CURLIB
Firewall . . . . . > *YES          *YES, *NO, *SAME
Journal . . . . . *NO              *YES, *NO, *SAME
Process all mail through MSF . . *NO      *YES, *NO, *SAME
Percent routing character . . .  *YES      *YES, *NO, *SAME
```

Figure 153. Change SMTP Attributes

4.5.3 Verifying the HOME400 TCP/IP domain name information

Enter the Change TCP/IP Domain (**CHGTCPDMN**) command. In the Host name search priority field, type ***LOCAL**. Searching priority ***LOCAL** causes the AS/400

system to look at the host table entries first, before querying the DNS. Figure 154 shows the configuration values in the CHGTCPDMN command (or CFGTCP option 12).

```

Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name . . . . . HOME400

Domain name . . . . . domain.com

Host name search priority . . . *LOCAL      *REMOTE, *LOCAL, *SAME

Internet address . . . . . 10.100.1.7

```

Figure 154. CHGTCPDMN - Search priority *LOCAL

4.5.4 Handling multiple SMTP domains on a single AS/400 system

The objective of this section is to set up the AS/400 system so that MFS recognizes that it is listening for the multiple SMTP domain names. In our example, we have three mail domains referred to as *domain1.com*, *domain2.com*, and *domain3.com*. Each company has its own distinct domain name. You *must* add three IP addresses and add three host table entries for the SMTP mail domain names.

Follow this procedure for each IP address on your AS/400 system:

1. On a command line, type CFGTCP. Press Enter.
2. Enter option 1 to add your TCP/IP address.
3. Enter option 10 to add one host table entry.
4. Associate the IP address with the mail domain on the host table entries.

Your host table should appear as shown in Figure 155.

```

Work with TCP/IP Host Table Entries
System: HOME400

Type options, press Enter.
 1=Add  2=Change  4=Remove  5=Display  7=Rename

Internet      Host
Opt  Address   Name

 10.100.1.3   domain1.com
 10.100.1.4   domain2.com
 10.100.1.5   domain3.com
 127.0.0.1    LOOPBACK
              LOCALHOST

```

Figure 155. Associating an IP address with the mail domain

The three IP interfaces do not have to be started. They are only needed because the SMTP server looks on the host table to see which domain names are handled by the AS/400 IP addresses.

These three IP addresses can also be virtual IP. See Appendix B, “Using virtual IP addresses” on page 329, for a further explanation.

Tip

To verify that the AS/400 system is listening for a mail domain on a specific IP address, type `netstat *ifc` on a command line. Then, type `5` in front of the IP addresses you defined. The first line shows the domain associated with the interface.

4.5.5 Adding the firewall name to the host table entries

For the SMTP server to resolve the mail router name defined in the SMTP attributes (Figure 153 on page 122), you *must* configure a host table entry for the firewall.

Specify the **INTERNAL* IP address for IBM Firewall for AS/400 (interface E, Figure 120 on page 102). Specify the internal secure IP address IBM eNetwork Firewall for Windows NT (interface B, Figure 129 on page 109). Figure 156 shows the TCP/IP host table configuration (CFGTCP option 10).

```
Work with TCP/IP Host Table Entries                                System:  HOME400
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  7=Rename

  Internet      Host
  Opt Address    Name

      192.168.2.2  fw2mail
                        fw2mail.domain.com

(If you use the Windows NT firewall put this entry instead)
      10.100.1.2  fw2nt
                        fw2nt.domain.com
```

Figure 156. Firewall configuration on the AS/400 TCP/IP host table

4.5.6 Starting the SMTP server

To start the SMTP server, complete these tasks:

1. Start the SMTP server by typing this command:

```
STRTCPSVR SERVER(*SMTP)
```

2. Verify that the Mail Server Framework (MSF) is running.

Use the `WRKACTJOB` command to determine if the mail server framework is running. Look in subsystem `QSYSWRK` for jobs named `QMSF`. If the `QMSF` job is not running, use the Start Mail Server Framework (`STRMSF`) command to start it.

The configuration of the SMTP server is now ready.

4.6 Configuring the POP3 server on the AS/400 system

This section describes the tasks that you must perform to install and configure a POP3 server on the AS/400 HOME400. The POP server is a simple store-and-forward mail system. It provides electronic mailboxes on the AS/400 system, from which clients can retrieve mail. It uses the AnyMail/400 mail server framework and the system distribution directory to process and distribute e-mail. It uses simple mail transfer protocol (SMTP) to forward mail.

4.6.1 Task summary

The following list summarizes the tasks used to implement the POP3 server on an AS/400 system:

1. Set up the POP3 server attributes.
2. Add POP3 accounts.
3. Configure POP3 accounts.
4. Start the POP3 server.

4.6.2 Setting up the POP3 server attributes

This section takes you through the steps for setting up the POP3 server attributes. Follow these steps:

1. On an AS/400 command line, type:

```
CHGPOPA
```

2. Press **F4**.

3. You *must* enter ***YES** in the Allow standard POP3 connection field. This tells the POP3 server that you are using a standard POP (TCP/IP) connection. We recommend setting the Message split size to ***NOMAX**.

4. Enter the correct values as shown in Figure 157, and press Enter.

Change POP Server Attributes (CHGPOPA)

Type choices, press Enter.

Autostart servers	*YES	*YES, *NO, *SAME
Number of initial servers . . .	3	1-20, *SAME, *DFT
Inactivity timeout	600	10-65535 seconds, *SAME, *DFT
Message split size	*NOMAX	32-2048 kilobytes, *SAME...
MIME CCSID:		
Coded character set identifier	00819	*SAME, *DFT, 00819, 00912...
When to use	*BESTFIT	*SAME, *BESTFIT, *ALWAYS
Allow standard POP connection .	*YES	*SAME, *YES, *NO
Host server connection	*NONE	*SAME, *NONE, *ALL, *IP...
+ for more values		
Address book:		
Enabled	*NO	*SAME, *NO, *YES
Refresh interval		1-65535 minutes, *NONE

Figure 157. Change POP Server Attributes

4.6.3 Adding POP3 accounts

If your POP3 users are already AS/400 users, skip to 4.6.4, “Configuring POP3 accounts” on page 126. Follow these steps:

1. To create a new user profile on an AS/400 command line, type:

```
CRTUSRPRF
```

2. Press **F4**.

For security reasons, you may use the INLMNU (*SIGNOFF) parameter. This means that the user is not allowed to sign on to the AS/400 system.

3. Enter the correct values for the user. Use the example shown in Figure 158 as a guide. After you enter the correct values, press Enter.

```
                                Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . gaelle      Name
User password . . . . . *****  Name, *USRPRF, *NONE
Set password to expired . . . . . *NO      *NO, *YES
Status . . . . . *ENABLED      *ENABLED, *DISABLED
User class . . . . . *USER      *USER, *SYSOPR, *PGMR...
Assistance level . . . . . *SYSVAL  *SYSVAL, *BASIC, *INTERMED...
Current library . . . . . *CRIDFT   Name, *CRIDFT
Initial program to call . . . . . *NONE  Name, *NONE
  Library . . . . .              Name, *LIBL, *CURLIB
Initial menu . . . . . *SIGNOFF    Name, *SIGNOFF
  Library . . . . . *LIBL        Name, *LIBL, *CURLIB
Limit capabilities . . . . . *NO     *NO, *PARTIAL, *YES
Text 'description' . . . . . 'Gaelle Jenni - POP3 account'
```

Figure 158. Creating a POP3 account

4.6.4 Configuring POP3 accounts

To configure a POP3 account on an AS/400 system, add an entry in the system distribution directory for each user. For users who do *not* have a directory entry, follow these steps:

1. On an AS/400 command line, type:

```
WRKDIRE
```

Press Enter. The display shown in Figure 159 on page 127 appears.

```

Work with Directory Entries

Type options, press Enter.
  1=Add      2=Change  4=Remove  5=Display details  6=Print details
  7=Rename   8=Assign different ID to description  9=Add another description

Opt  User ID  Address  Description
  1
    *ANY     HOME400  Generic entry for HOME400
    DHQB     HOME400  operations userid
    FSTEELE  HOME400  Fant Steele
    QDFTOWN  QDFTOWN  Default Owner
    QDOC     QDOC     Internal Document Owner
    QLPAUTO  QLPAUTO  Licensed Program Automatic User
    QLPINSTL QLPINSTL Licensed Program Install
    QNOTES   QNOTES   LOTUS NOTES INTEGRATION PROFILE

```

Figure 159. Work with Directory Entries

2. Type 1, and then press Enter. The display shown in Figure 160 appears. In this redbook, we include only the relevant parameters in Figure 160, Figure 161, and Figure 162 on page 128.

```

Add Directory Entry

Type choices, press Enter.

User ID/Address . . . . GAELE HOME400
Description . . . . . Gaelle Jenni - POP3 Account
System name/Group . . . HOME400 F4 for list
User profile . . . . . GAELE F4 for list
Network user ID . . . .

```

Figure 160. Add Directory Entry (Part 1 of 2)

3. Press the Page Down key three times or until you arrive at the display shown in Figure 161.

```

Add Directory Entry

Type choices, press Enter.

Mail service level . . 2
                                                                1=User index
                                                                2=System message store
                                                                4=Lotus Domino
                                                                9=Other mail service

For choice 9=Other mail service:
Field name . . . . . F4 for list

Preferred address . . . 3
                                                                1=User ID/Address
                                                                2=O/R name
                                                                3=SMTP name
                                                                9=Other preferred address
                                                                F4 for list

Address type . . . . .
For choice 9=Other preferred address:
Field nam

```

Figure 161. Add Directory Entry (Part 2 of 2)

4. Enter the values shown in Figure 161. Press **F19** (Add name for SMTP). The display shown in Figure 162 appears.

```

                                Add Name for SMTP
                                System:  HOME400

Type choices, press Enter.

User ID . . . . . :  GAELE
Address . . . . . :  HOME400

SMTP user ID . . . . .  gaelle
SMTP domain . . . . .  domain1.com

SMTP route . . . . .

```

Figure 162. Adding an SMTP user ID and domain

5. Fill in the SMTP user ID and SMTP domain fields. These values are combined to form the SMTP e-mail address for this user (gaelle@domain1.com). Press Enter.
6. To confirm your choice, press Enter again.

For users who *have* a directory entry, follow these steps:

1. On an AS/400 command line, type:

```
WRKDIRE
```

Press Enter. The display shown in Figure 163 appears.

```

                                Work with Directory Entries

Type options, press Enter.
  1=Add      2=Change  4=Remove  5=Display details  6=Print details
  7=Rename  8=Assign different ID to description  9=Add another description

Opt  User ID  Address  Description
-----
    *ANY      HOME400  Generic entry for HOME400
    DHQB      HOME400  operations userid
    FSTEELE   HOME400  Fant Steele
  2  GAELE    HOME400 Gaelle Jenni - POP3 Account
    QDFTOWN   QDFTOWN  Default Owner
    QDOC      QDOC     Internal Document Owner
    QLPAUTO   QLPAUTO  Licensed Program Automatic User
    QLPINSTL  QLPINSTL Licensed Program Install

```

Figure 163. Work with Directory Entries

2. Type 2, and then press Enter. The display shown in Figure 164 appears. In this redbook, we include only the relevant parameters in Figure 164 and Figure 165 on page 129.

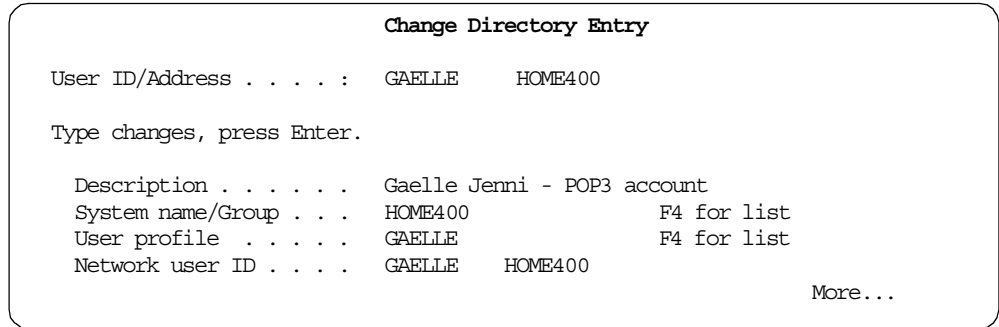


Figure 164. Change Directory Entry (Part 1 of 2)

3. Press the Page Down key four times or until you arrive at the display shown in Figure 165.

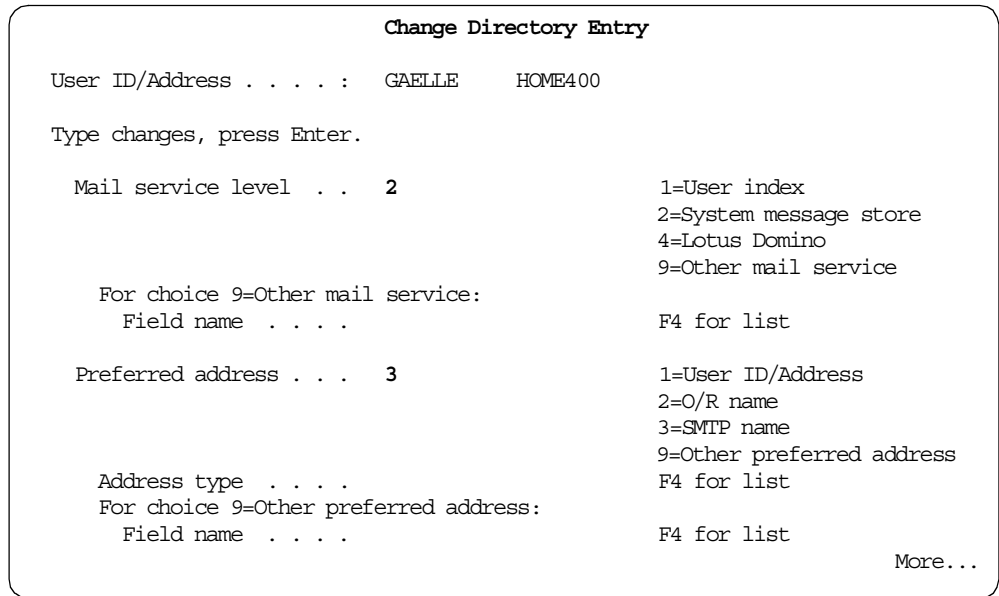


Figure 165. Changing Directory Entry (Part 2 of 2)

4. Enter the values shown in Figure 165. Press **F19** (Add name for SMTP). The display shown in Figure 166 on page 130 appears.

```

Change Name for SMTP
System: HOME400
User ID/Address . . . . . : GAELLE HOME400

Type choices, press Enter.

SMTP user ID . . . . . gaelle
SMTP domain . . . . . domain1.com

SMTP route . . . . .

```

Figure 166. Add SMTP user ID and domain

5. Fill in the SMTP user ID and SMTP domain fields. These values are combined to form the SMTP e-mail address for this user (gaelle@domain1.com). Press Enter.
6. To confirm your choice, press Enter again.

4.6.5 POP3 mailboxes

Once there is an entry in the system distribution directory for a POP mail user, the mailbox for that user is created automatically. This happens either the first time the client logs on successfully or when mail is received for the client.

4.6.6 Starting the POP3 server

To start the POP3 server, complete the following tasks:

1. Enter the following command:


```
STRTCPSVR SERVER(*POP)
```
2. Verify that the MSF is running.

Use the `WRKACTJOB` command to determine if the mail server framework is running. Look in subsystem `QSYSWRK` for jobs named `QMSF`. If the `QMSF` job is not running, use the Start Mail Server Framework (`STRMSF`) command to start it.

The configuration of the POP3 server is now ready.

4.7 Configuring the Domino server for mail

The task you must perform to set up the Domino server for this scenario is similar to the task documented in 3.7, “Configuring the Domino server for mail” on page 71. In this section, we refer you to that procedure and only document the steps that are different for this scenario.

4.7.1 Task summary

The following list summarizes the tasks used to implement the Domino server on the AS/400 HOME400:

1. Plan the Domino server on an AS/400 system.
2. Set up HOME400 to handle Domino.
3. Install the Domino server on HOME400.
4. Install Domino Administrator on your workstation.
5. Set up your workstation to administer Domino.
6. Configure Domino server for SMTP mail.
7. Link the Domino server with the firewall.
8. Create Lotus Notes mail users.

Perform the procedures from 3.7.2, “Planning the Domino server on an AS/400 system” on page 71, through 3.7.6, “Setting up your workstation to administer Domino” on page 78. This guides you from task 1 through task 5 from the task list above. Return here when you reach “Stop here” on page 82.

4.7.2 Configuring Domino server for SMTP mail

This section describes how to set up the Domino server to handle SMTP mail. On the Domino Administrator desktop, perform the following steps. Use the example shown in Figure 167 as a guide for the first five steps.

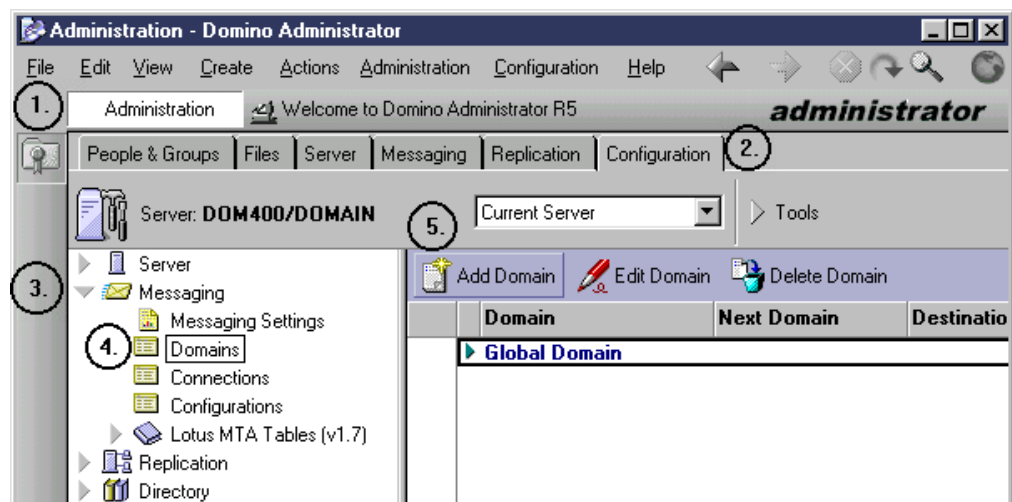


Figure 167. Domain document

1. Click the **Administration** button (1).
2. Click the **Configuration** tab (2).
3. Open **Messaging** in the navigation tree (3).
4. Click **Domains** (4).
5. Click the **Add Domain** button (5). The display shown in Figure 168 on page 132 appears.

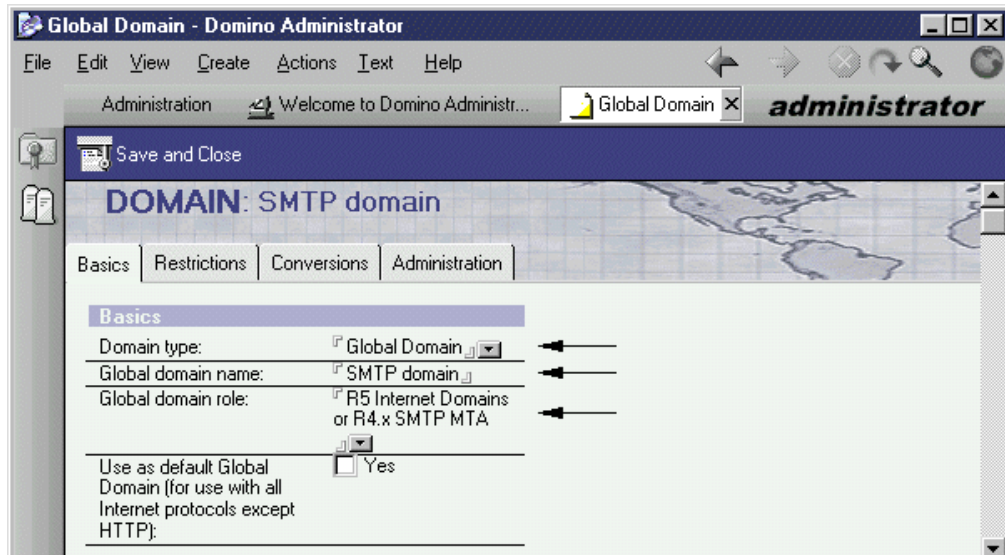


Figure 168. Domain document - Basics

6. Select **Global Domain** for Domain type.
7. Enter **SMTP Domain** for Global domain name.
8. Select **R5 Internet Domains** for Global domain role.
9. Click on the **Conversions** tab. The window shown in Figure 169 appears.

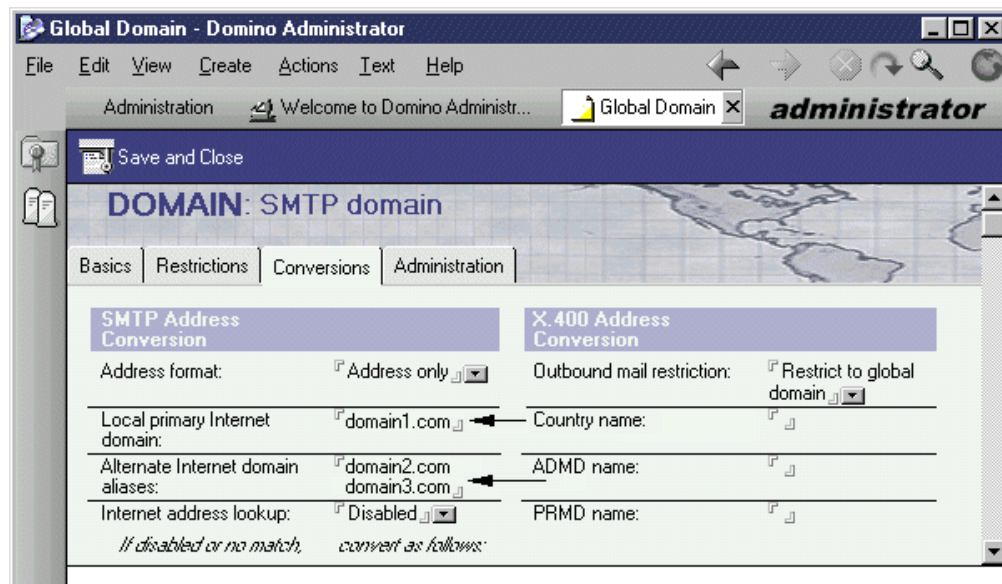


Figure 169. Domain document - Conversion

10. Enter **domain1.com** for Local primary Internet domain.
11. Enter **domain2.com** and **domain3.com** for Alternate Internet domain aliases.
12. Click **Save and Close**. You return to a window similar to the window shown in Figure 167 on page 131.

Use Figure 170 on page 133 as a guide for the next three steps.

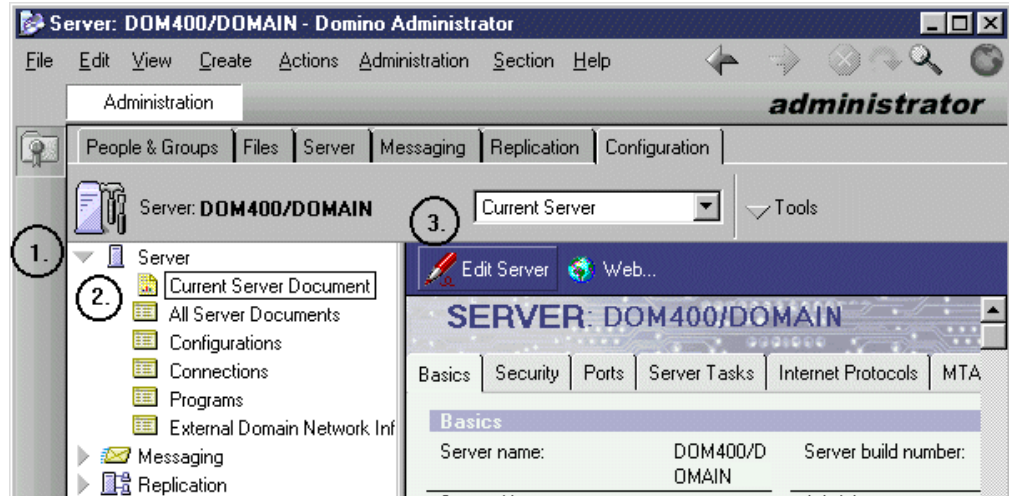


Figure 170. Server document

13. Open **Server** in the navigation tree (1).
14. Select **Current Server Document** (2).
15. Click the **Edit Server** button (3). The window shown in Figure 171 appears.

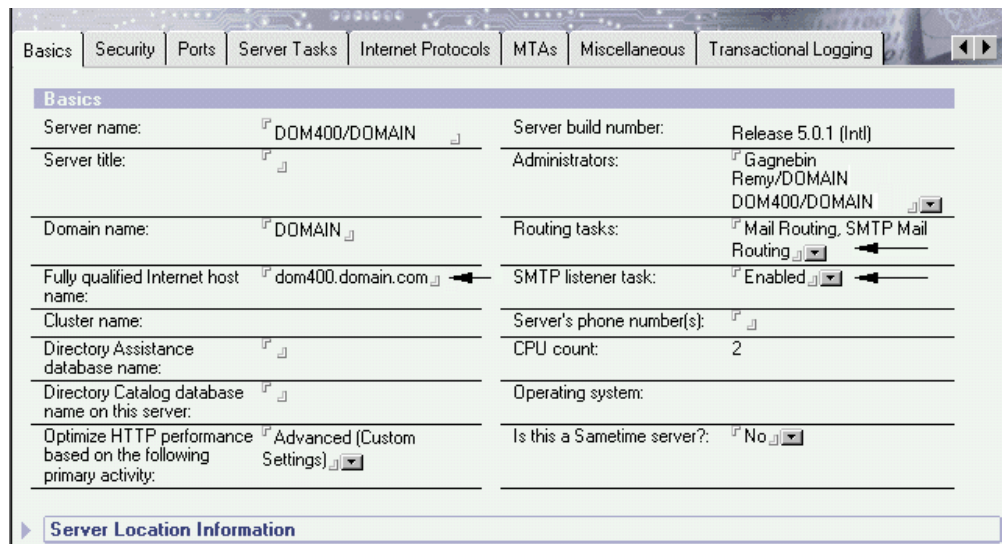


Figure 171. Server document - Basics

16. Verify that the fully qualified Internet host name matches the Domino server name.
17. Verify that the SMTP listener task is set to `Enabled`.
18. Verify that the Routing tasks are `Mail Routing` and `SMTP Mail Routing`.
19. Click **Save and Close**.

You have now configured the Domino server to handle multiple SMTP domains.

4.7.3 Linking Domino server with the firewall

To link the Domino SMTP server with the firewall, perform the following steps. Use the example shown in Figure 172 as a guide for the first three steps.

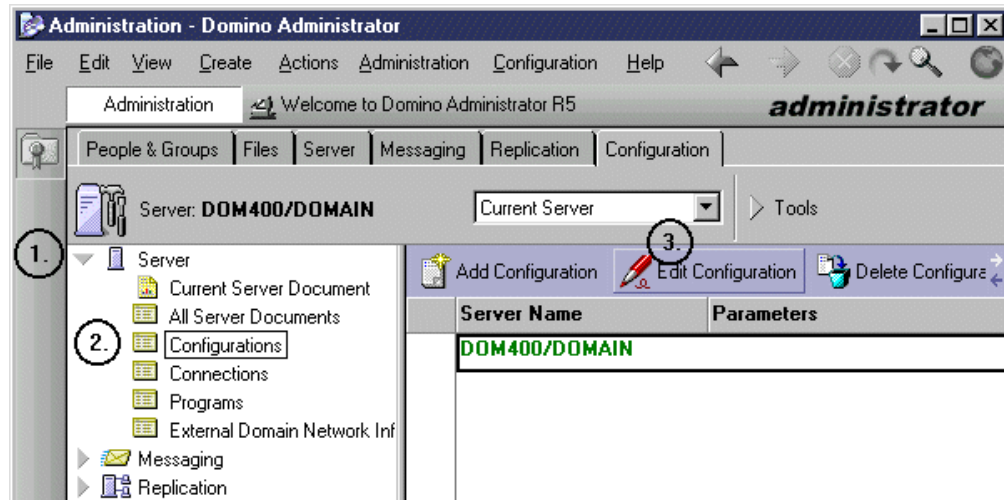


Figure 172. Configuration document

1. Open **Server** in the navigation tree (1).
2. Select **Configurations** (2).
3. Click the **Edit Configurations** button (3). The window shown in Figure 173 appears.

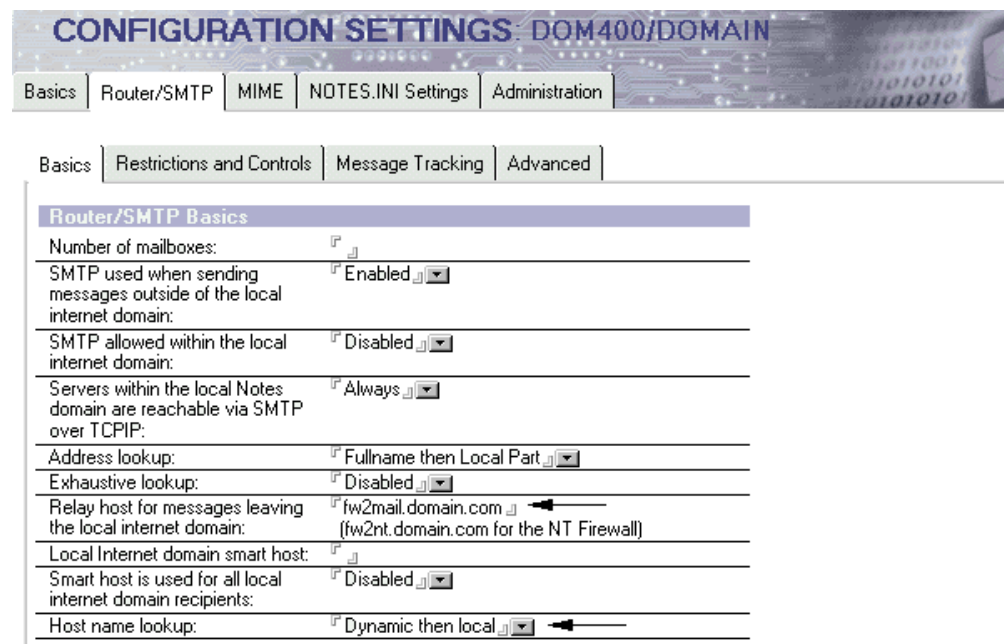


Figure 173. Configuration document - Router/SMTP

4. Click the **Router/SMTP** tab.

5. Enter the firewall name for Relay host for messages leaving the local Internet domain. Figure 173 shows the AS/400 firewall and the NT firewall name. In your configuration, you should only have one entry.
6. Verify that the Host name lookup is set to `Dynamic` then `local`.
7. Click **Save and Close**.

You have now linked the Domino SMTP server with the SMTP relay function of your firewall.

4.7.4 Creating Lotus Notes mail users

The Domino server is now ready to receive mail from the Internet. In this section, we create a Lotus Domino user and their mailbox. To build the user and mailbox, perform the following steps. Use the example shown in Figure 174 as a guide for the first five steps.

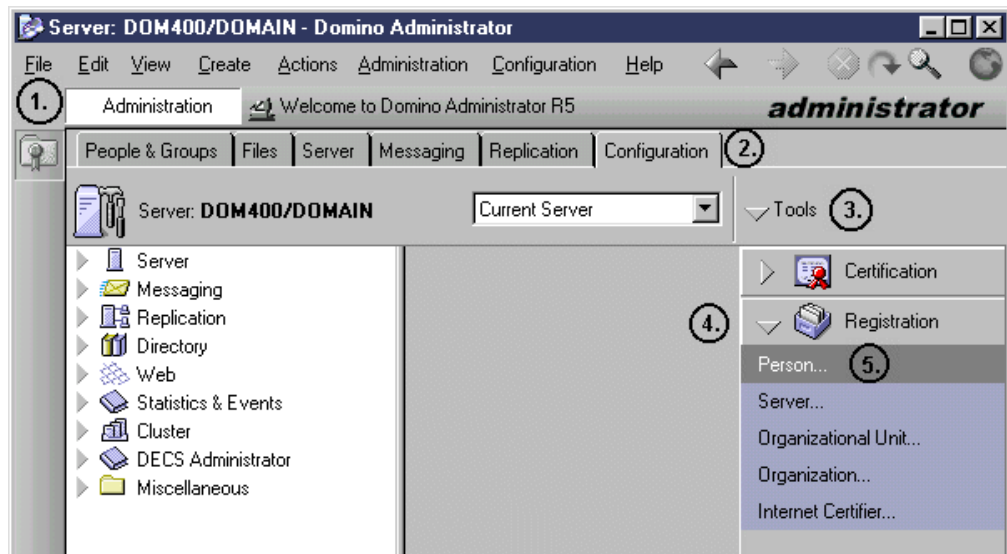


Figure 174. Registration - Person

1. On the Domino Administrator desktop, click **Administration** (1).
2. Click the **Configuration** tab (2).
3. Click the **Tools** pull-down menu (3).
4. Click **Registration** (4).
5. Click **Person** (5). The display shown in Figure 175 appears.

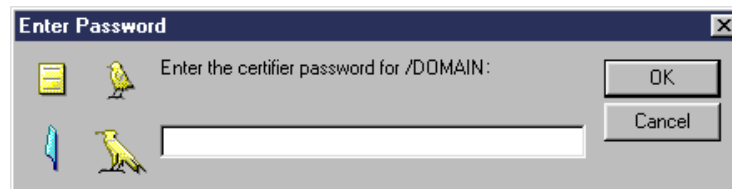


Figure 175. Certifier ID password

6. Enter the password, and then click **OK**. The display shown in Figure 176 on page 136 appears. Use the figure to complete the next five steps.

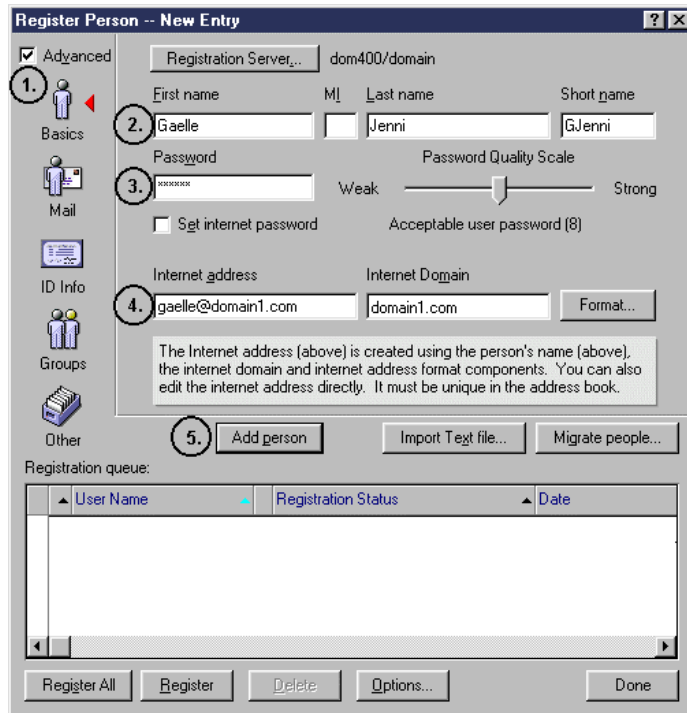


Figure 176. Register Person (Part 1 of 2)

7. Check **Advanced** (1).
8. Enter the person's first name and last name (2).
9. Enter the person's password (3).
10. Enter the person's Internet address and Internet domain (4).
11. Click the **Add person** button (5). The display shown in Figure 177 on page 137 appears.

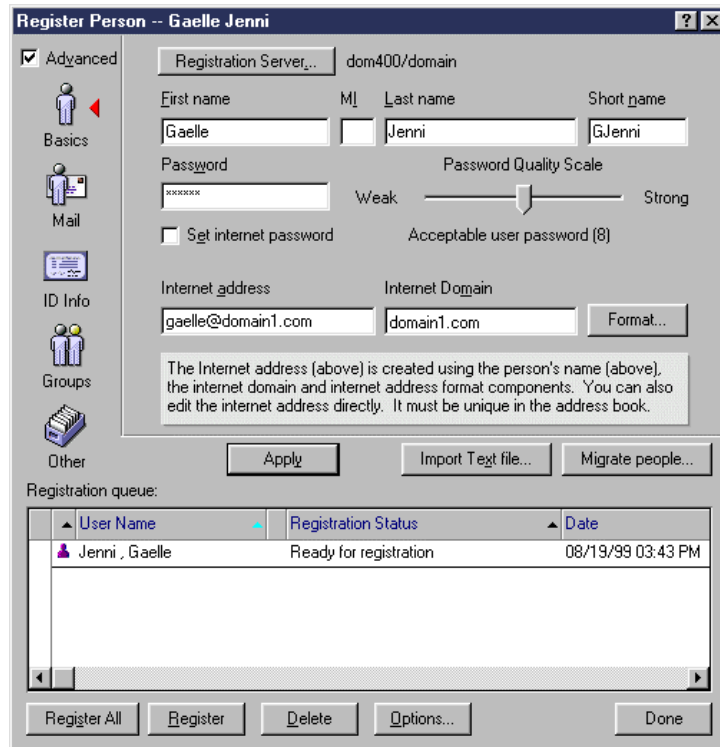


Figure 177. Register Person (Part 2 of 2)

12.Repeat steps 8 through 11 to add the next two users.

13.Click the **Register All** button.

The registration process can take several minutes.

You have now successfully registered your users and mailboxes. The user ID for each person is stored on the Domain's Public Address Book.

The last step you need to do is to configure Lotus Notes on your PCs. If you never before configured Lotus Notes for your mail, refer to the Lotus documentation that came with the product.

Chapter 5. Multiple domains on multiple systems

This chapter presents the procedures for configuring firewalls that support a mail environment composed of multiple domains. Each domain is processed by one mail server. The procedures described here include setting up the configuration of both IBM Firewall for AS/400 and IBM eNetwork Firewall for Windows NT. This chapter also contains the procedures that we use to set up an SMTP and POP3 server on one AS/400 system and SMTP and Domino servers on two AS/400 systems.

5.1 Scenario

In this scenario, we present a company that has multiple AS/400 systems. Each system has its own AS/400 system with its own mail domain. The public mail domains and the private mail domains are the same.

The internal DNS can be on any AS/400 system on the network. In our scenario, the AS/400 HOME400 handles this function. The mail servers are configured as follows:

- SMTP with POP3 server on the AS/400 MAILSRV3.
- Domino server using SMTP on a Domino server on AS/400 HOME400.
- Domino server using SMTP on an AS/400 system on AS/400 MAILSRV2.

The firewall is either IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT

If you want to open the firewall to allow POP3 or Domino clients to access the internal mail server from the Internet, refer to 3.3.5, "Planning NAT to map the POP3 server address outside the firewall" on page 33, through 3.3.10, "Filter rules to allow Domino access from the Internet" on page 38, for IBM Firewall for AS/400. Refer to 3.4.5, "Planning NAT to map POP3 server address outside the firewall" on page 51, through 3.4.9, "Creating a service" on page 56, for IBM eNetwork Firewall for Windows NT.

5.1.1 Scenario network configuration

Figure 178 on page 140 illustrates a logical view of the network configuration used in this scenario.

There are three ways to implement the firewall:

- The firewall is an Integrated Netfinity Server running IBM Firewall for AS/400.
- The firewall is a separate PC running Windows NT Server and IBM eNetwork Firewall for Windows NT.
- The firewall is an Integrated Netfinity Server running IBM eNetwork Firewall for Windows NT.

The procedure for setting up Windows NT Server on an Integrated Netfinity Server is provided in Chapter 8, "Installing a Windows NT Server to support firewalls" on page 289.

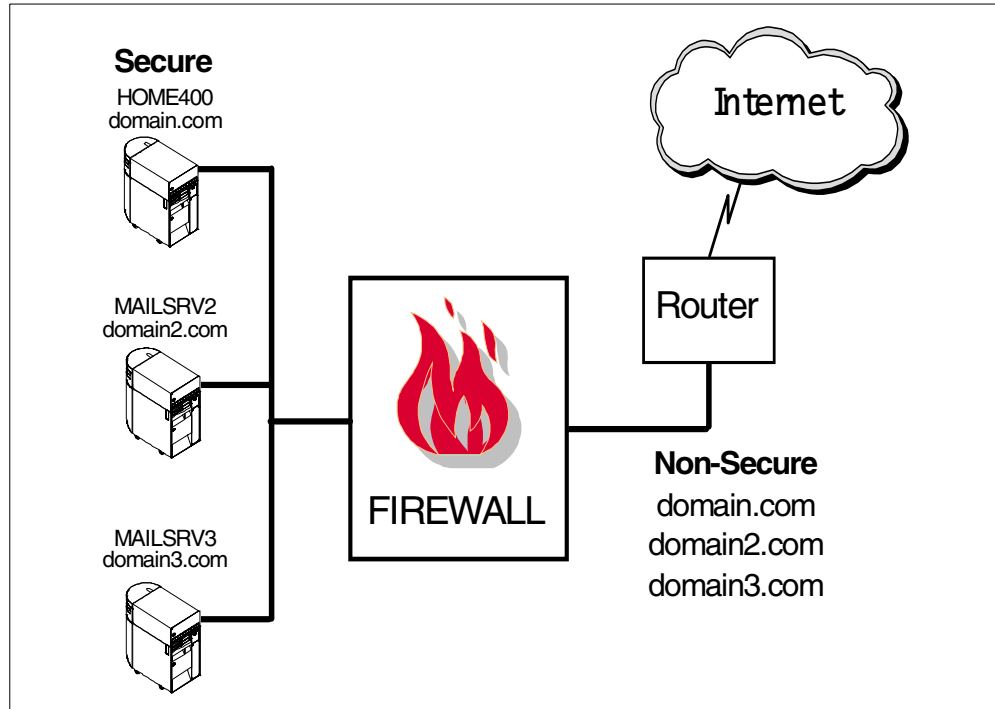


Figure 178. Scenario network configuration for multiple domains on a single server

5.1.2 Scenario objectives

The objectives of this scenario are:

- Configure the IP domains on the internal DNS.
- Configure the firewall so that it can handle the mail domains.
- Configure HOME400 to handle Domino server with SMTP running on a Domino server for internal and Internet mail.
- Configure the MAILSRV2 to handle Domino server with SMTP running on the AS/400 system for internal and Internet mail.
- Configure the MAILSRV3 to handle an SMTP and POP3 server for internal and Internet mail.

5.1.3 Scenario advantages

This scenario has the following advantages:

- The firewall can be either IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT.
- IBM Firewall for AS/400 can handle the DNS function, so you do not need to spend extra money to handle this function by your ISP or on other DNS in the DMZ.

5.1.4 Scenario limitations

There are also some limitations associated with this scenario. They include:

- The DNS function of IBM eNetwork Firewall for Windows NT uses the NT DNS in a cache-only mode, which means that a DNS is needed in the DMZ or you will have to use the DNS of your ISP (using the ISP DNS may mean extra fees).
- Inbound mail is processed in three different systems. If you want to run an antivirus system for scanning mail coming from the Internet, you have to route it from the firewall to a specific server and then distribute it to mail servers from this server.

5.1.5 Planning considerations

Consider the following points when planning to implement:

- Is there any internal DNS in your company?
- Are the PCs configured to handle an internal DNS?
- Are you using IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT as your firewall?

The remainder of this chapter documents the procedures used to set up the firewall and mail server using both firewall products and both mail products. You should choose the sections that are appropriate for your environment.

- FW3MAIL refers to IBM Firewall for AS/400.
- FW3NT refers to IBM eNetwork Firewall for Windows NT.
- HOME400 refers to the AS/400 system on domain *domain.com*.
- MAILSRV2 refers to the AS/400 system on domain *domain2.com*.
- MAILSRV3 refers to the AS/400 system on domain *domain3.com*.
- DOM400 refers to the Domino server on AS/400 HOME400.
- DOMINO2 refers to the Domino server on AS/400 MAILSRV2.

Table 16 lists the domain names, host names, and IP addresses used for this scenario.

Table 16. Domain names, host names, and IP addresses

Domain name	Host name	IP address
domain.com	fw3nt (non-secure)	208.222.150.250
domain.com	fw3nt	10.100.1.2
domain.com	fw3mail (non-secure)	208.222.150.250
domain.com	fw3mail	10.100.1.2
domain.com	fw3mail (internal LAN)	192.168.2.2
domain.com	home400	10.100.1.7
domain.com	home400 (internal LAN)	192.168.2.1
domain.com	dom400	10.100.1.8

Domain name	Host name	IP address
domain2.com	mailsrv2	10.100.1.9
domain2.com	domino2	10.100.1.10
domain3.com	mailsrv3	10.100.1.11
(Host table entry)	domain.com	10.100.1.3
(Host table entry)	domain2.com	10.100.1.4
(Host table entry)	domain3.com	10.100.1.5

Table 17 lists the values used to configure the AS/400 DNS for this scenario using different SMTP servers.

Table 17. Secure mail server name - DNS MX values

Firewall product	Secure domain name	MX value for mail server name for AS/400 SMTP	MX value for mail server name for Domino SMTP
IBM Firewall for AS/400	domain.com		dom400.domain.com.
	domain2.com	mailsrv2.domain2.com.	
	domain3.com	mailsrv3.domain3.com.	
IBM eNetwork Firewall for Windows NT	domain.com		dom400.domain.com.
	domain2.com	mailsrv2.domain2.com.	
	domain3.com	mailsrv3.domain3.com.	

Table 18 lists the values used to configure SMTP mail relay on the firewall for this scenario using the different firewall and mail products.

Table 18. Domain name and secure mail server name - Firewall values

Firewall product	Secure and public domain name	Firewall mail server name for AS/400 SMTP	Firewall mail server name for Domino SMTP
IBM Firewall for AS/400	domain.com		domain.com
	domain2.com	domain2.com	
	domain3.com	domain3.com	
IBM eNetwork Firewall for Windows NT	domain.com		dom400.domain.com
	domain2.com	mailsrv2.domain2.com	
	domain3.com	mailsrv3.domain3.com	

In Table 19, list the domain names, host names, and IP addresses that you need for this scenario.

Table 19. User values for domain name, host name and IP address

Domain name	Host name	IP address
(Host table entry)		
(Host table entry)		
(Host table entry)		

In Table 20, list the values you need to configure the AS/400 DNS for this scenario.

Table 20. User values for secure mail server name - DNS MX values

Firewall product	Secure domain name	MX value for mail server name for AS/400 SMTP	MX value for mail server name for Domino SMTP

In Table 21, list the values you need to configure the SMTP mail relay on the firewall for this scenario.

Table 21. User values for domain name and secure mail server name - Firewall

Firewall product	Secure and public domain name	Firewall mail server name for AS/400 SMTP	Firewall mail server name for Domino SMTP

5.1.6 Task summary

To set up this scenario, you must configure the DNS to support the mail environment (step 1), configure a firewall (step 2 or 3), and configure your mail servers (steps 3, 5, and 6):

1. Configure the AS/400 DNS.
2. Configure IBM Firewall for AS/400 (FW3MAIL).
3. Configure IBM eNetwork Firewall for Windows NT (FW3NT).
4. Configure the SMTP and POP3 server on the AS/400 MAILSRV3.
5. Configure the Domino server for mail on the AS/400 DOM400.
6. Configure the Domino server for mail on the AS/400 MAILSRV2.

5.2 Configuring the AS/400 DNS

This section describes the tasks that you must perform to configure the internal AS/400 DNS to handle multiple domains on a single mail server. If the DNS is not already installed, refer to *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147.

5.2.1 Task summary

To configure the AS/400 DNS for this scenario, perform the following steps:

1. Configure the AS/400 DNS to handle the internal domains.
2. Add a host name to the domains.
3. Configure the MX record for each domain.
4. Configure the internal DNS to forward the queries to the firewall.

5.2.2 Configuring the AS/400 DNS to handle internal domains

To configure the AS/400 DNS, use Operations Navigator, which is included as part of Client Access Express for Windows.

To access the DNS configuration, select your **AS/400 system name-> Network->Server->TCP/IP**. Double-click **DNS**. Click the + symbol beside the DNS Server - Home400 (system name) entry. The display shown in Figure 179 appears.

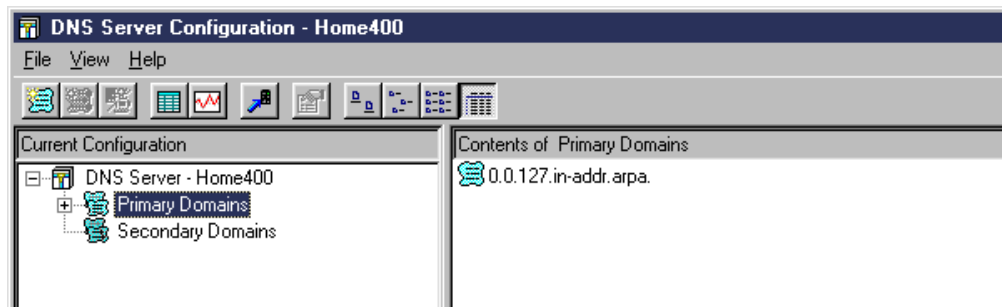


Figure 179. Configuring the AS/400 DNS to handle the internal domain: domain.com

To add a primary domain, perform the following procedure:

1. Right-click on **Primary Domains**. Select **New Primary Domain**. The display shown in Figure 180 on page 145 appears.

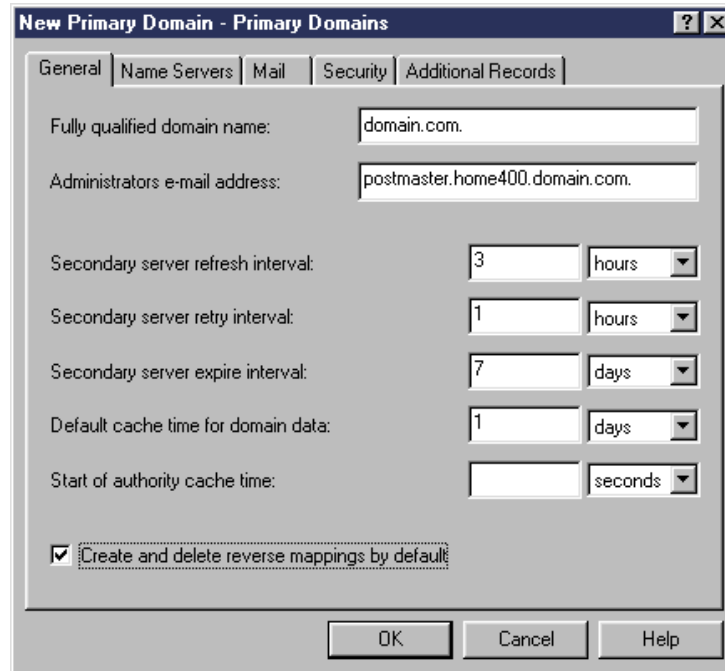


Figure 180. New Primary Domain domain.com

2. Enter the domain name `domain.com`. You *must* put a dot at the end of your domain since it is a fully qualified domain name.
3. Check **Create and delete reverse mappings by default**.
4. Click **OK**. The display shown in Figure 181 appears. Your domain name is displayed in the right-hand frame.
5. Right-click on the domain name you added. A drop-down menu appears. Click **Enable**. This enables the domain in the DNS.

You have now created the domain `domain.com`.

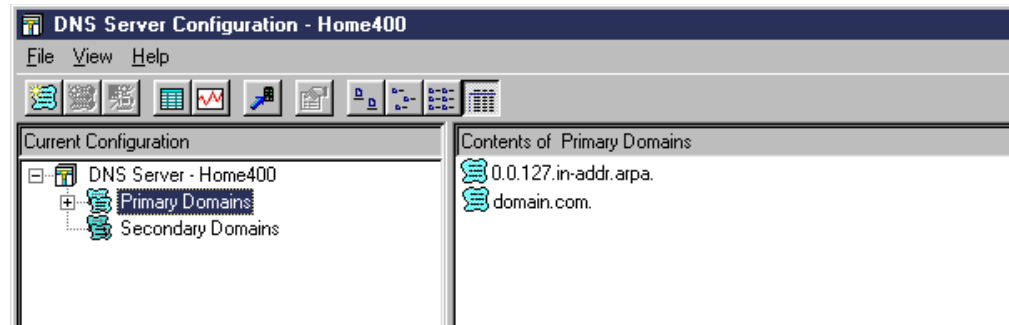


Figure 181. Content of Primary Domains after creating domain.com

Repeat the steps in this section to create `domain2.com` and `domain3.com`.

When you have completed adding all the domains, your DNS Server Configuration window should look similar to the example shown in Figure 182 on page 146. As a result of configuring our scenario, we have the following domains:

- 0.0.127.in-addr.arpa Reverse lookup for loopback domain 127.0.0
- 1.100.10.in-addr.arpa Reverse lookup for 10.100.1 domain
- domain.com Domain for domain.com
- domain2.com Domain for domain2.com
- domain3.com Domain for domain3.com

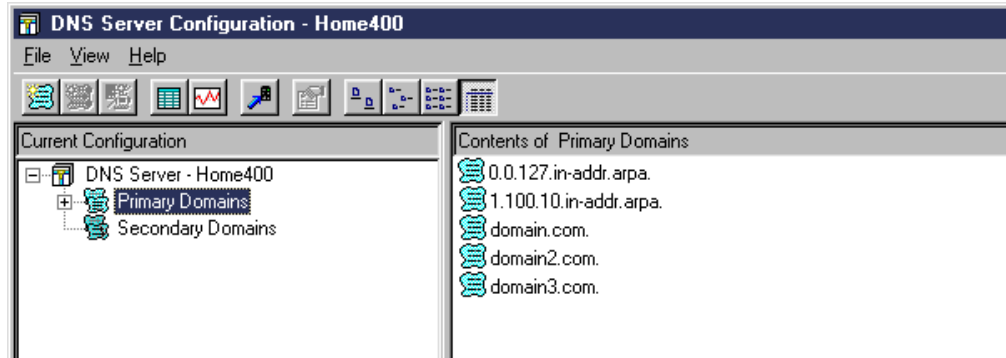


Figure 182. Content of Primary Domains after creating the three domains

If any of the domain names have a yellow exclamation mark (!) on them, they need to be enabled. Right-click on the domain name. A drop-down menu appears. Click **Enable**. This enables the domain in the DNS.

You have now added the domain names to the DNS. You should continue setting up the DNS.

5.2.3 Adding host names to the domains

After you create the domains, you need to add the host names to each domain. Refer to Figure 182 to start this procedure. To add the Host names, perform the following steps:

1. Right-click on the domain name to which you want to add the host name.
2. Select **New Host**.
3. Click **Add**. The New Host window is displayed (Figure 183).

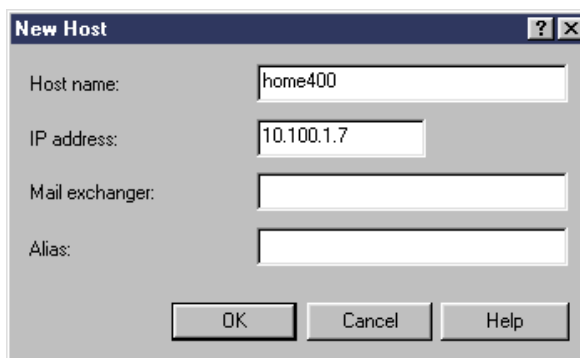


Figure 183. Adding the AS/400 host name

4. Enter the host name and the IP address.
5. Click **OK**.

Repeat the steps in this section to add all the host names for all the domains. See Table 16 on page 141. Only the host names that have a 10.100.1.x IP address need to be stored in the DNS.

Now you need to add the mail exchange (MX) information for each of the mail domains.

5.2.4 Configuring the MX record for each domain

The MX record tells the DNS client (it can be either a PC or another DNS) the name of the SMTP server that processes mail for the domain. Refer to Figure 182 on page 146 to start this procedure. To add the MX records, perform the following steps:

1. Right-click the domain name that you want to configure.
2. Select **Properties**.
3. Click the **Mail** tab.
4. Click **Add**. The display shown in Figure 184 appears.

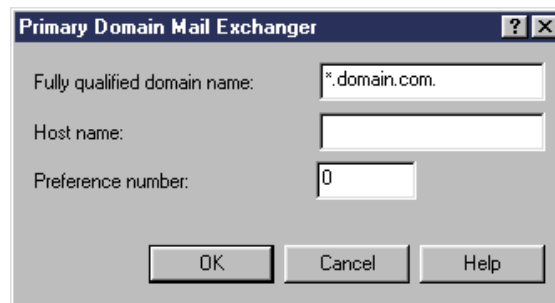


Figure 184. Adding an MX record in a domain

5. Remove the asterisk (*) from the front of the default domain name. In our example, we changed (*.domain.com.) to domain.com.
6. Enter the fully qualified host name of the SMTP server. Refer to Table 17 on page 142 for the MX record value that refers to the domain. Be sure to include the dot (.) at the end of the host name.
7. Click **OK**.
8. Click **OK** a second time to exit the Properties window.

Repeat the steps in this section to create an MX record for domains *domain2.com* and *domain3.com*.

5.2.5 Configuring the internal DNS to forward the queries to the firewall

The internal DNS cannot answer the queries that are intended for the Internet. It needs to be linked with the DNS firewall.

If e-mail is sent to somebody@us.ibm.com, it first goes to the internal SMTP server. Then, it is forwarded to the firewall. From the firewall, it is sent to the Internet.

To set up DNS forwarding, you must change the DNS properties. Start at the DNS Server Configuration window shown in Figure 185 on page 148.

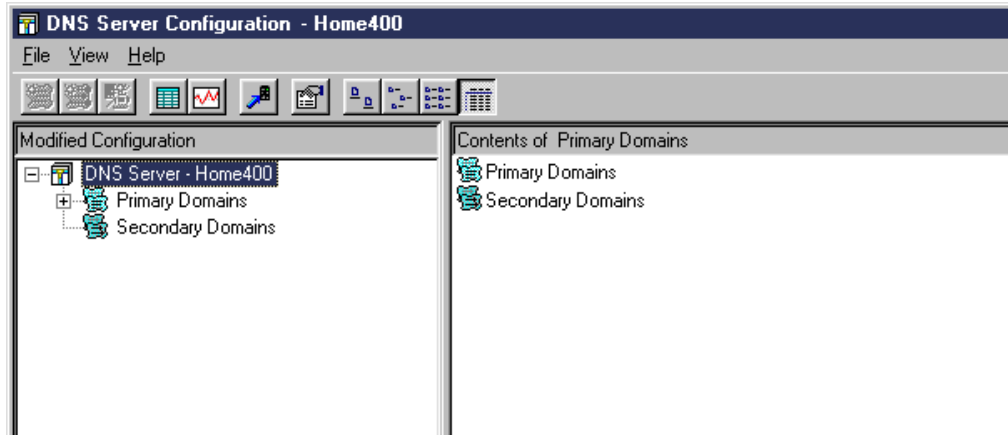


Figure 185. Configuring the internal DNS to forward queries to the firewall

Use the following procedure to change the properties of the DNS:

1. Right-click **DNS Server - Home400**.
2. Select **Properties**.
3. Click the **Forwarders** tab. The display shown in Figure 186 appears.

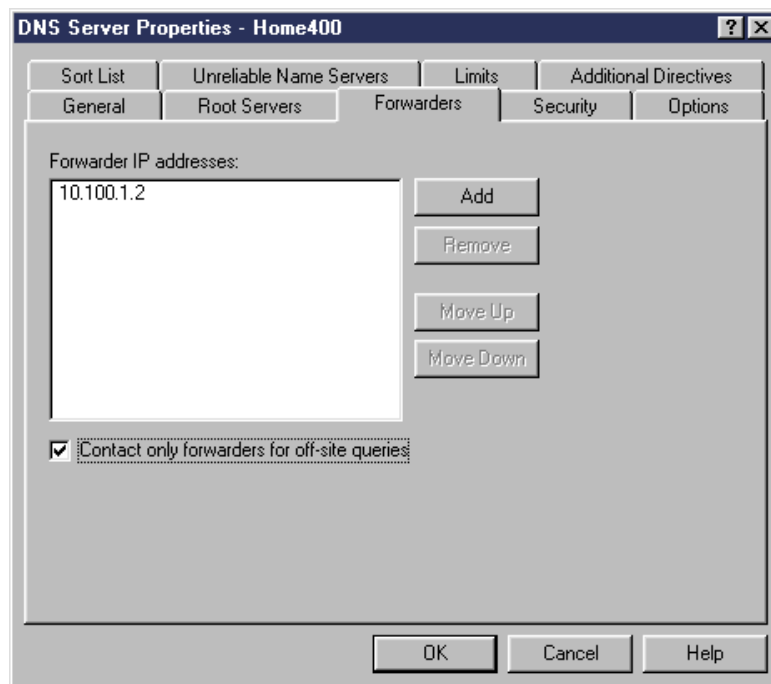


Figure 186. Adding the IP address of the firewall to the forwarders list

4. Click the **Add** button.
5. Enter the secure IP address of the firewall.
6. Check **Contact only forwarders for off-site queries**.
7. Click **OK**.

The DNS configuration is now ready to handle your SMTP mail. Stop and start the DNS server, or click **File->Update Server** to update the DNS server configuration and make your configuration available.

5.3 Configuring IBM Firewall for AS/400 (FW3MAIL)

This section describes the tasks that you must perform to configure IBM Firewall for AS/400 to handle multiple domains on multiple mail servers.

5.3.1 Scenario network configuration

Figure 187 shows the network configuration used in this scenario. In this portion of the scenario, we use an Integrated Netfinity Server to run IBM Firewall for AS/400. The network diagram would be the same if we use IBM eNetwork Firewall for Windows NT. The *Internal LAN and one LAN adapter make up the secure side of the Network. The other LAN adapter is used to connect to the ISP router.

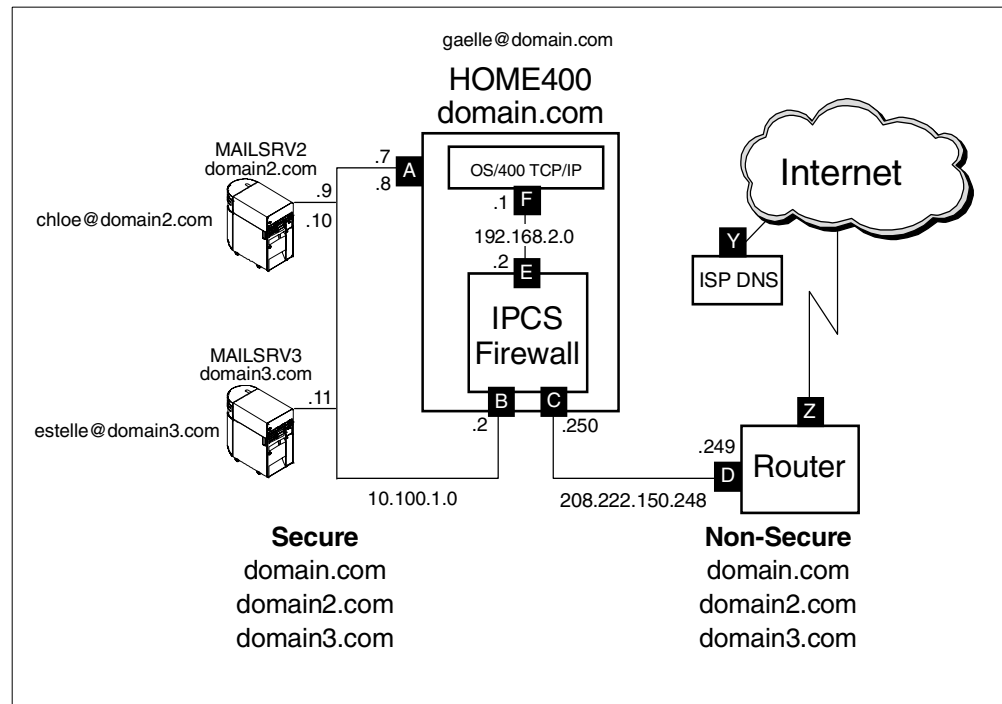


Figure 187. Multiple domains on multiple mail servers with IBM Firewall for AS/400

5.3.2 Task summary

The following list summarizes the tasks used to configure IBM Firewall for AS/400:

1. Install IBM Firewall for AS/400.
2. Perform the basic configuration.
3. Remove the MX record for domain *domain.com*

5.3.3 Installing IBM Firewall for AS/400 (FW3MAIL)

Install the firewall at the local site using the instructions in the manual *Getting Started with IBM Firewall for AS/400*, SC41-5424. A summary of the installation parameters is shown on the Complete the Firewall Installation summary page in Figure 188.

Complete the Firewall Installation

Review the information that you have entered. Make any changes on this page. When you are sure that the information is correct, click the **Install** button to complete the firewall installation. This step takes several minutes to run. Please be patient.

Firewall Name	FW3MAIL							
Firewall Resource Name	CC02							
Router IP Address	208	222	150	249				
Route Destination	Subnet Mask		Next Hop					
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>					
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>					
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>					
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>					
	Port 1	Port 2						
LAN Type	Token Ring (16Mb)	Token Ring (16Mb)						
Adapter Address	400000000037	4000000000250						
IP Address	10	100	1	2	208	222	150	250
Subnet Mask	255	255	255	0	255	255	255	248

Figure 188. Firewall Installation summary page (FW3MAIL)

Start the firewall by clicking **Start** (Figure 189).

Start the Firewall

The firewall takes several minutes to start. Please be patient. Click **Start** to start the firewall.

Figure 189. Starting the firewall (FW3MAIL)

5.3.4 Performing basic configuration (FW3MAIL)

Perform the basic configuration of the local firewall. For further information, refer to *Getting Started with IBM Firewall for AS/400*, SC41-5424 and *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162.

In the *Review Configuration*, be aware that the *Secure Mail Server* and the *Secure Domain* refer to the internal mail domain name. The SMTP domain name in the inbound e-mail (the value to the right of the @ symbol) is changed to the value in the Secure Mail Server column. This value must match the SMTP mail address setup for the user on the secure mail server. In our scenario, these values have to be exactly the same because of the domain names we select for our internal users. The value in the Secure Mail Server parameter is used in an MX record DNS query to find the SMTP server that processes the mail. If the query fails, an A record DNS query is done for the value. If an IP address is returned, the mail is routed to the mail server. In most cases, it is easiest to use the same value for the Secure Mail Server and the Secure Domain parameters and let the internal DNS MX records point to the secure mail server system. Refer to Table 18 on page 142 for information about the domain name and secure mail server name.

If you do not have a DNS server in the secure network, this technique will not work. You must specify the fully qualified name of the secure mail server (for example, `hostname.domain.com`) in the Secure Mail Server column. This means that the e-mail address of the users will be in the form `userid@hostname.domain.com`.

In this configuration, we create the three mail domains needed during the basic configuration. This is an easy way to create a domain in IBM Firewall for AS/400.

We recommend that you link the firewall DNS with multiple DNS servers in the outside world. If one fails, you can still continue to send e-mail and surf the Web. In our scenario, the three DNS servers belong to the ISP.

For more information about IBM Firewall for AS/400, refer to Appendix D, "Firewall concepts" on page 349.

Figure 190 on page 152 and Figure 191 on page 153 show the review configuration for FW3MAIL (refer to Figure 187 on page 149 for the scenario network configuration). Complete these tasks:

1. Review the information on the form. If all the information is correct, click **OK**. A confirmation page (Figure 192 on page 154) is shown. It indicates that the firewall is configured.
2. Read the message in the window. Click **Yes** to continue.



Review Configuration

Review the information that you have entered. Make any changes on this page. When you are sure that the information is correct, print the page for future reference. This creates all the firewall configuration settings. This may take a few minutes to run, so please be patient.

Your AS/400 is: HOME400.DOMAIN.COM

Your firewall is: FW3MAIL

Secure domain name servers:

10.100.1.7

Secure Port	IP Address	Subnet Mask
<input checked="" type="radio"/> Port 1	10.100.1.2	255.255.255.0
<input type="radio"/> Port 2	208.222.150.250	255.255.255.248

Secure Mail Server	Secure Domain	Public Domain
domain.com	domain.com	domain.com
domain2.com	domain2.com	domain2.com
domain3.com	domain3.com	domain3.com

Name Server	IP Address
dns1.isp.com	194.41.0.4
dns2.isp.com	128.9.0.107
dns3.isp.com	192.33.4.12

Figure 190. Basic firewall configuration summary page for FW3MAIL (Part 1 of 2)

Public Server	Public IP Address	Private IP Address

Services	Proxy	SOCKS	NAT
HTTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HTTPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FTP (passive)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FTP (active)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Telnet	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Secure Telnet		<input type="checkbox"/>	<input type="checkbox"/>
Gopher	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WAIS			<input type="checkbox"/>
IRC		<input type="checkbox"/>	<input type="checkbox"/>
RealAudio			<input type="checkbox"/>
Lotus Notes		<input type="checkbox"/>	<input type="checkbox"/>
LDAP		<input type="checkbox"/>	<input type="checkbox"/>
Secure LDAP		<input type="checkbox"/>	<input type="checkbox"/>
Server Mapper		<input type="checkbox"/>	<input type="checkbox"/>
DRDA		<input type="checkbox"/>	<input type="checkbox"/>
POP3 Mail		<input type="checkbox"/>	<input type="checkbox"/>
NNTP		<input type="checkbox"/>	<input type="checkbox"/>
Secure NNTP		<input type="checkbox"/>	<input type="checkbox"/>

If you selected any NAT services, then specify the translation of private to public IP addresses.

NAT	IP Address	Mask
Private	10.100.1.2	255.255.255.0
Public		

OK Cancel

Figure 191. Basic firewall configuration summary page for FW3MAIL (Part 2 of 2)

The firewall is now ready for you to perform the basic configuration. Click **Yes** (Figure 192 on page 154).

The Firewall is Configured

You have successfully configured the firewall. The next step is to restart the firewall servers so that your configuration changes take effect. This will only take a short time. Do you want to restart the firewall?

Figure 192. Confirmation that the firewall is configured

IBM Firewall for AS/400 configuration is now ready.

For more information about IBM Firewall for AS/400, refer to Appendix D, “Firewall concepts” on page 349.

5.4 Configuring IBM eNetwork Firewall for Windows NT (FW3NT)

This section describes the tasks that you must perform to configure the IBM eNetwork Firewall for Windows NT to handle multiple domains on multiple mail servers.

5.4.1 Scenario network configuration

Figure 193 shows the network configuration used in this scenario.

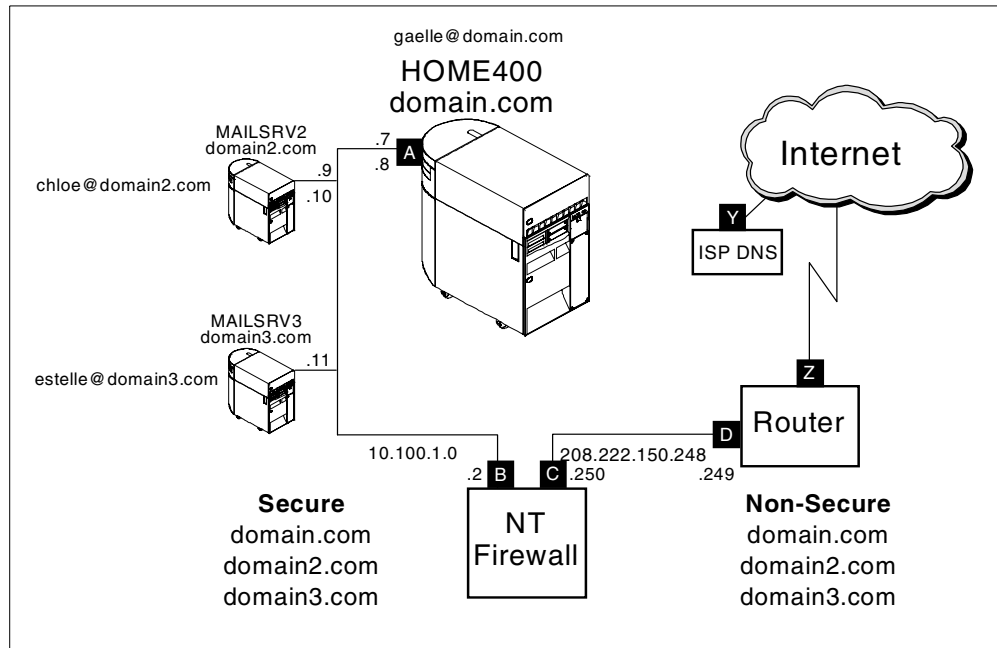


Figure 193. Multiple mail servers with IBM eNetwork Firewall for Windows NT

5.4.2 Task summary

The following list summarizes the tasks used to configure IBM eNetwork Firewall for Windows NT:

1. Install IBM eNetwork Firewall for Windows NT.
2. Setup IBM eNetwork Firewall for Windows NT.

5.4.3 Installing IBM eNetwork Firewall for Windows NT (FW3NT)

Install the firewall on the Windows NT PC using the instructions in *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT, SG24-5209*.

If you do not have this rebook and do not have Internet access to download it, complete the following steps:

1. Install the Windows NT server operating system.
2. Install the DNS Server for the Windows NT server.
3. Install Service Pack 4 for the Windows NT server. Use Service Pack 5 if it is available. Service Pack 4 is required. Do not install IBM eNetwork Firewall for Windows NT on the system without the Service Pack.
4. Create a local user with administrator authority.
5. Install the IBM NDIS intermediate driver.
6. Activate IP forwarding in the TCP/IP parameters.
7. Install the firewall product.

5.4.4 Setting up IBM eNetwork Firewall for Windows NT

Complete these steps to set up IBM eNetwork Firewall for Windows NT:

1. Run the **Configuration Client** in the IBM Firewall folder.
2. Log in with a user that has administrator authority.
3. To start basic configuration, click **Setup Wizard** in the Help menu (Figure 194).

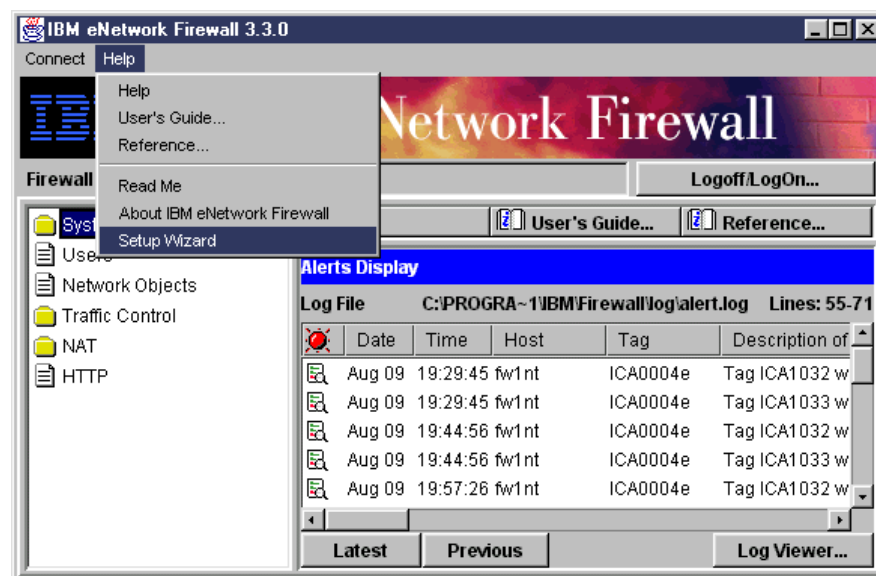


Figure 194. Starting firewall wizard

4. The Welcome window appears (Figure 195). Read the window carefully.

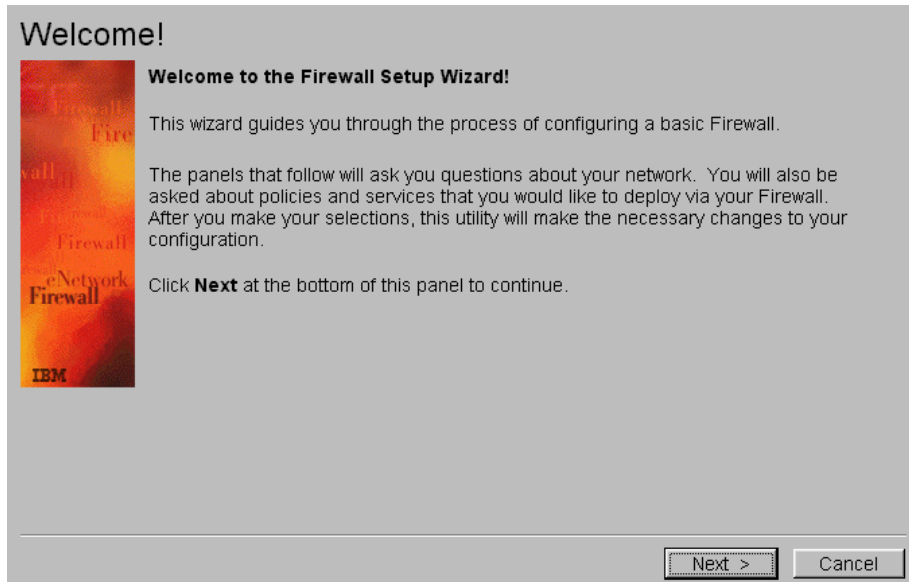


Figure 195. Welcome screen firewall wizard

5. Click **Next**. The window shown in Figure 196 appears. Read the window carefully.

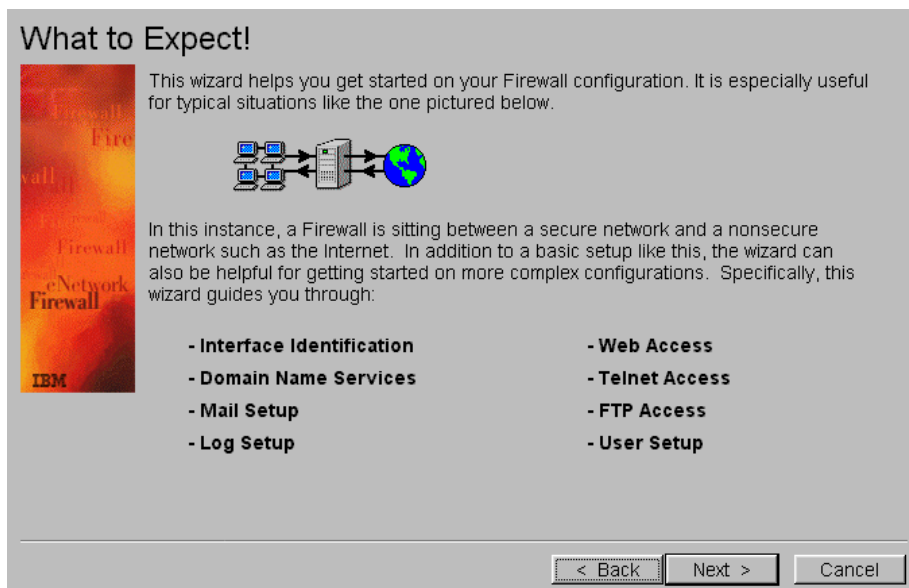


Figure 196. What to Expect firewall wizard

6. Click **Next**. The window shown in Figure 197 on page 157 appears. Read the window carefully.



Figure 197. Important notice firewall wizard

7. Click **Next**. The window shown in Figure 198 appears.

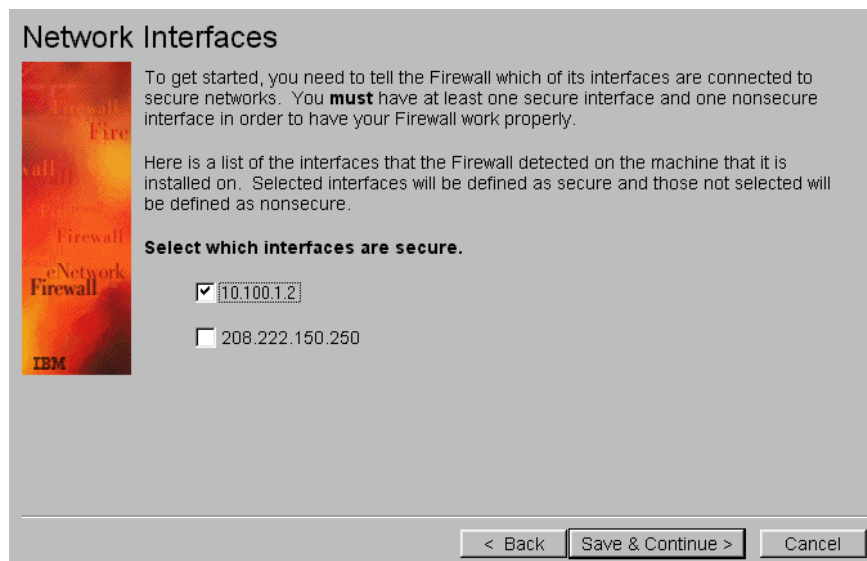


Figure 198. Network interface selection

8. Choose the secure interface. Click **Save & Continue**. The window shown in Figure 199 on page 158 appears.

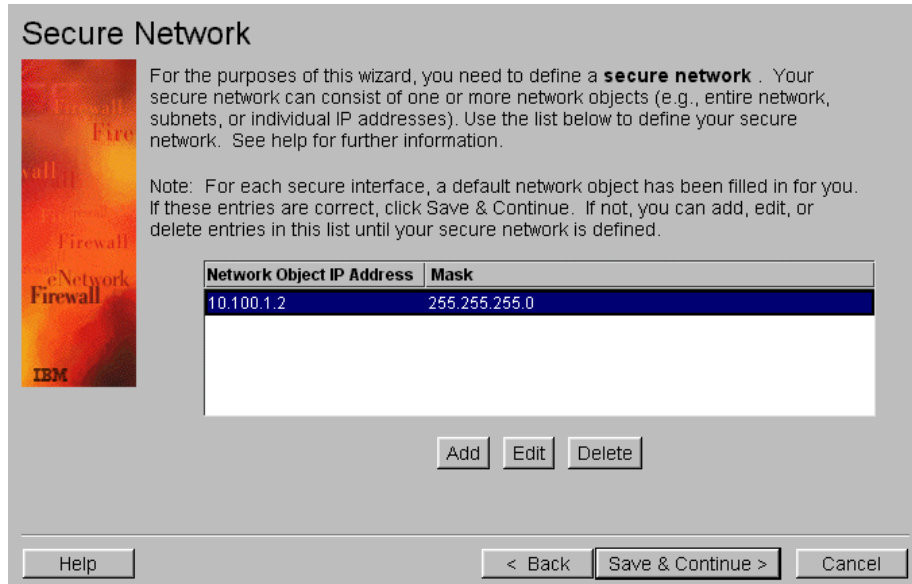


Figure 199. Secure Network configuration

- Define your secure network. In the window shown in Figure 199, the wizard is guessing that your secure network is any IP address that starts with 10.100.1. Click **Save & Continue**. The window shown in Figure 200 appears.

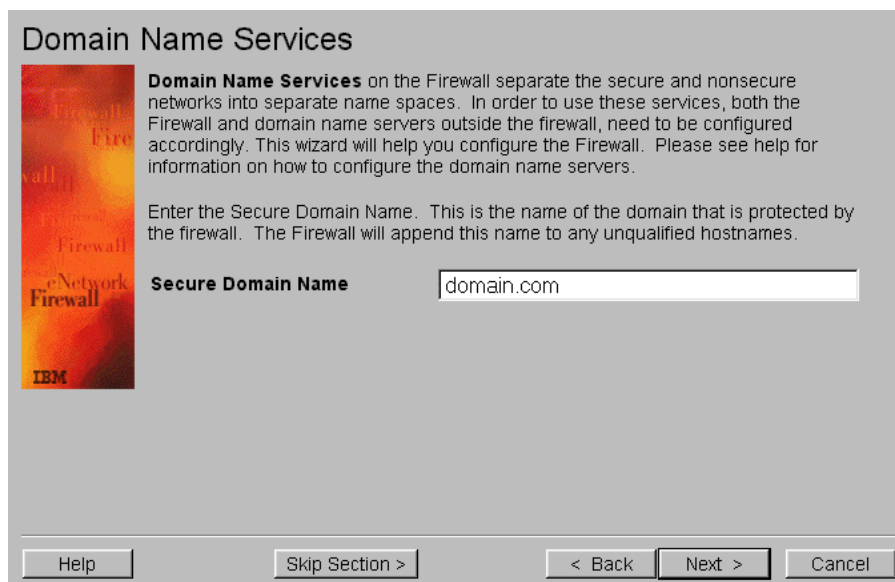


Figure 200. Domain Name Services

- Enter the name of your internal domain name. This domain is protected by your firewall. Click **Next**. The window shown in Figure 201 on page 159 appears.

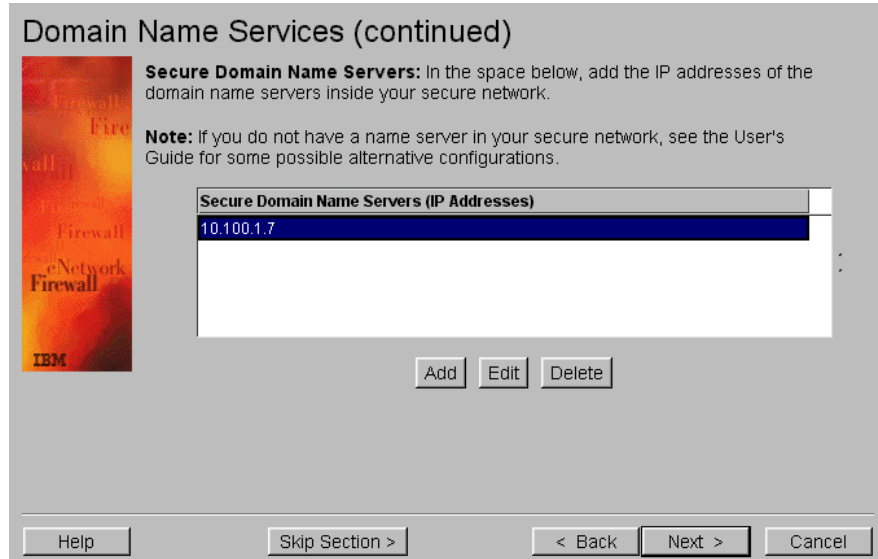


Figure 201. Secure DNS IP address

11. Enter the IP address of the secure internal DNS. Click **Next**. The window shown in Figure 202 appears.

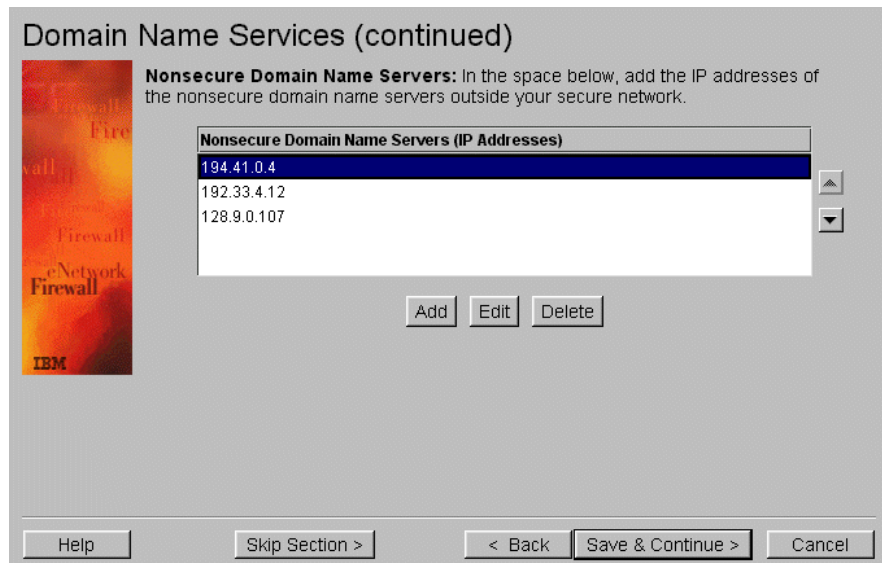


Figure 202. Non-secure DNS IP addresses

12. Click **Add**.
13. Enter the IP address of the non-secure DNS (ISP DNS). Click **Next**.
14. Repeat steps 12 and 13 if the firewall DNS is linked with more DNS (recommended).
15. Click **Save & Continue**. The window shown in Figure 203 on page 160 appears.

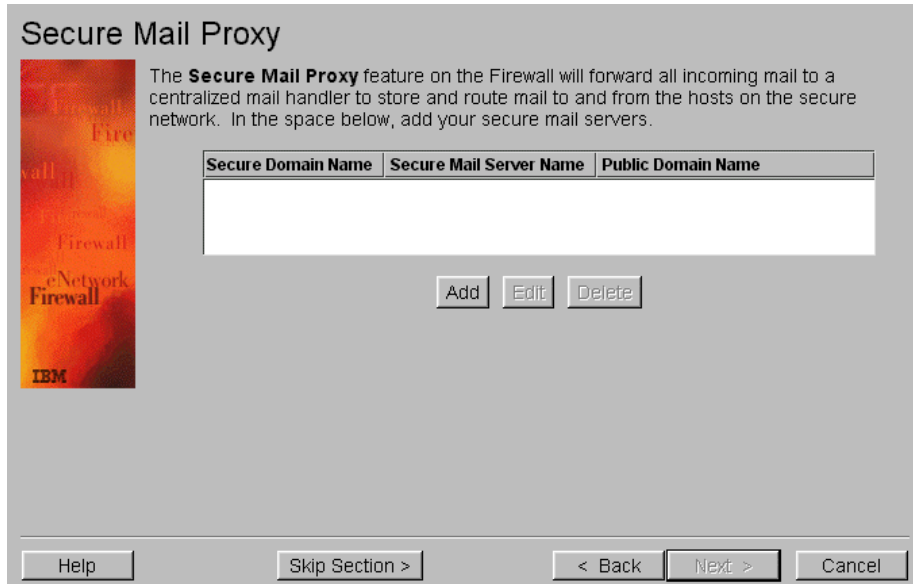


Figure 203. Secure Mail Proxy

16. Click **Add**. The window shown in Figure 204 appears.



Figure 204. Adding a secure mail server

17. Enter your Secure Domain Name, Secure Mail Server Name, and Public Domain Name. Refer to Table 18 on page 142 for information about domain names and secure mail server names. Click **Save & Continue**. The window shown in Figure 205 on page 161 appears.



Figure 205. Secure Mail Proxy

18. Repeat steps 16 and 17 for *domain2.com* and *domain3.com*.

19. Click **Next**. The window shown in Figure 206 appears.

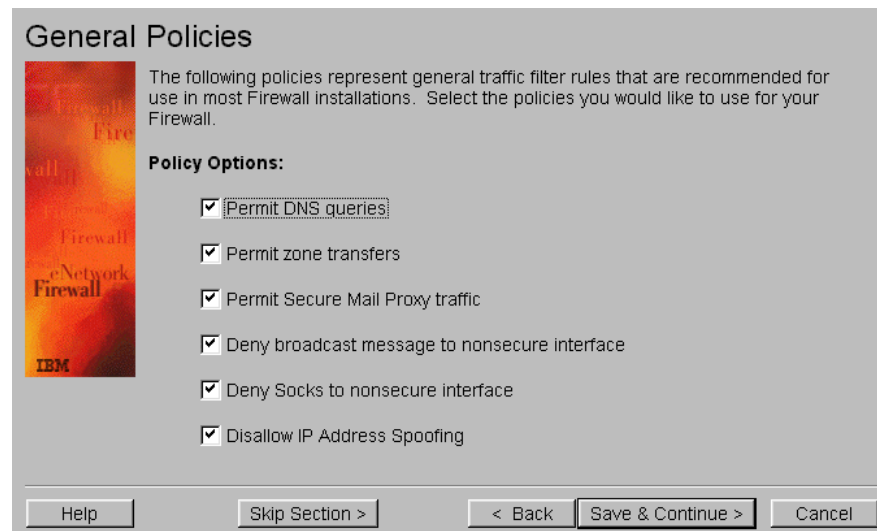


Figure 206. Security policies configuration

20. The marked options that you see under Policy Options are recommended for most firewall installations. Click **Save & Continue**. The window shown in Figure 207 on page 162 appears.



Figure 207. Web Access

21. Specify whether to allow Internet access to users. Click **Next**. The window shown in Figure 208 appears.

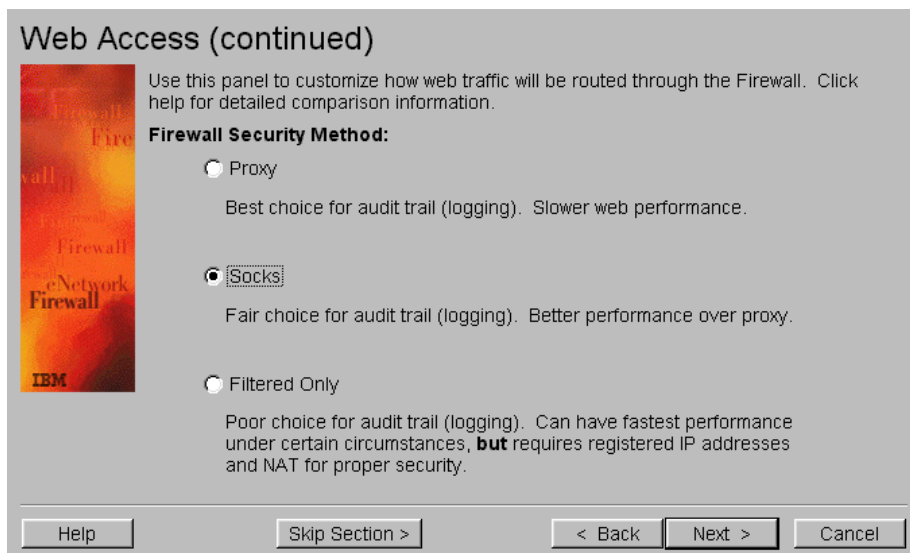


Figure 208. Web Access via Proxy, Socks, or Filtered Option

22. Specify the Web access option that matches best with your company. Click **Next**. The window shown in Figure 209 on page 163 appears.

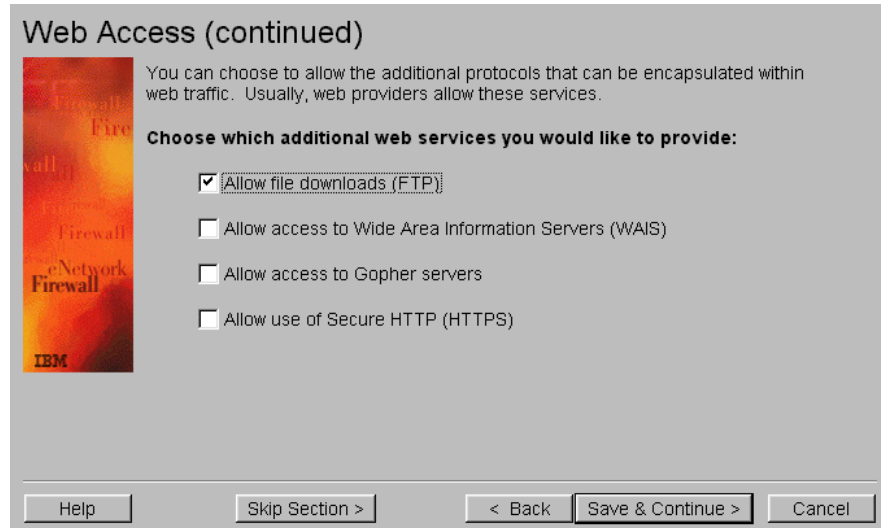


Figure 209. Web Access services

23. Select which services are allowed. Click **Save & Continue**. The window shown in Figure 210 appears.

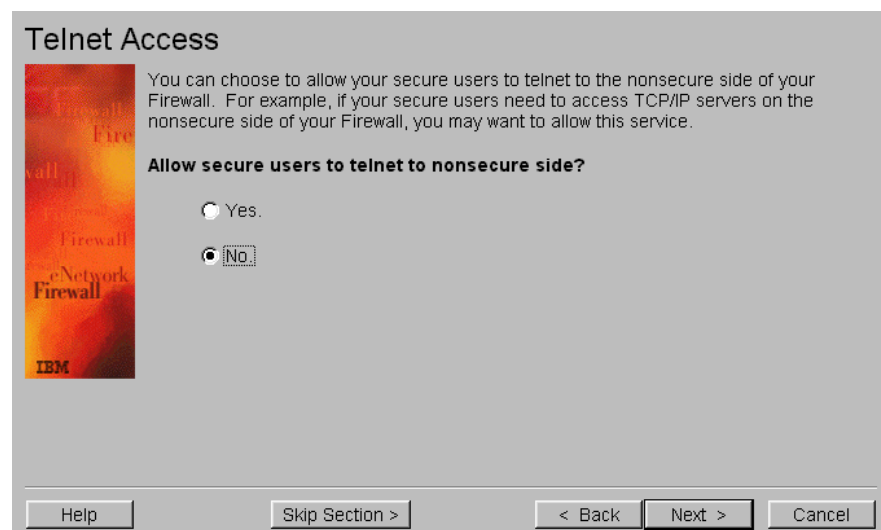


Figure 210. Telnet Access

24. Specify whether to allow Telnet access on the non-secure port of the firewall. Click **Next**. The window shown in Figure 211 on page 164 appears.

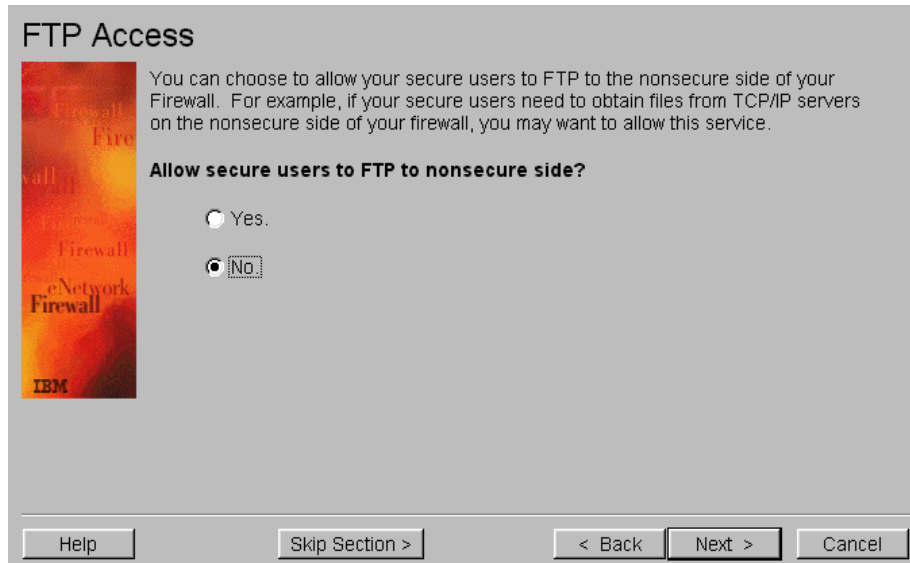


Figure 211. FTP Access

25. Specify whether to allow FTP access on the non-secure port of the firewall. Click **Next**. The window shown in Figure 212 appears.

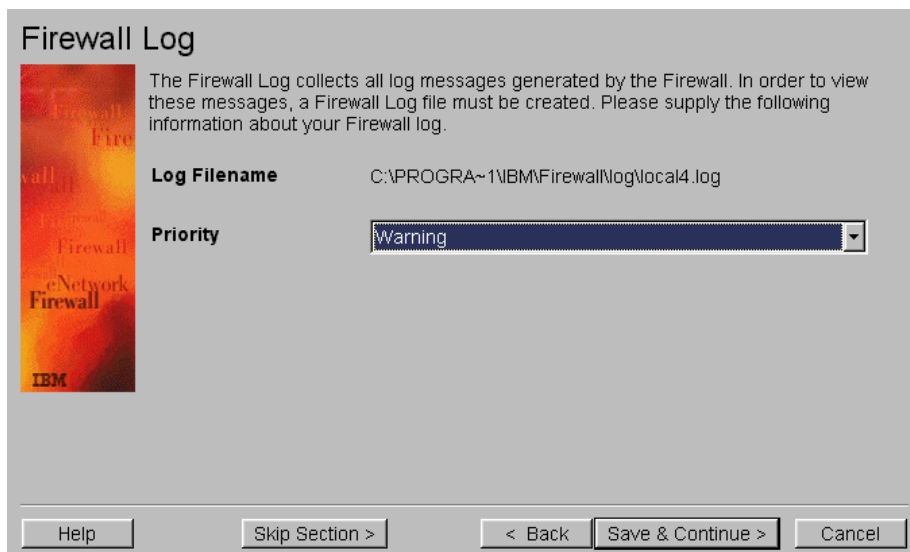


Figure 212. Firewall Log

26. Choose which level of logs are stored on the firewall database. Click **Save & Continue**. The window shown in Figure 213 on page 165 appears.

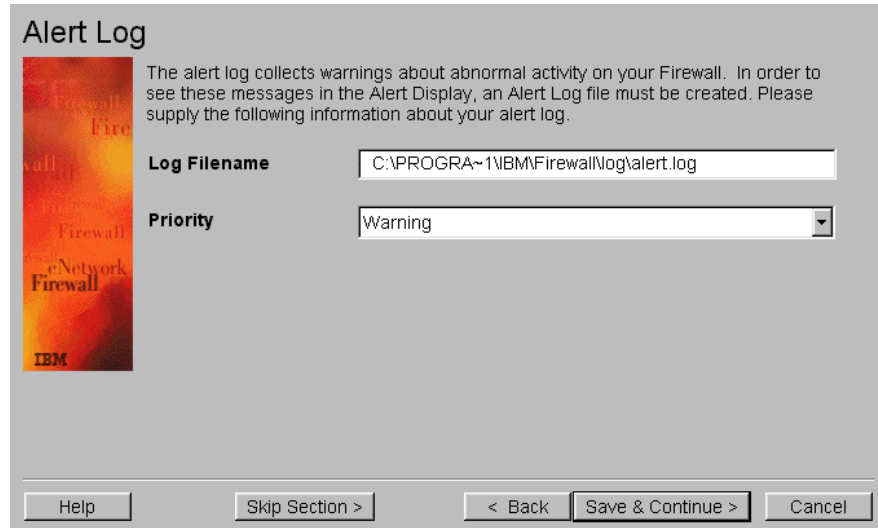


Figure 213. Alert Log

27. Choose which level of logs are stored on the alert database. Click **Save & Continue**. The window shown in Figure 214 appears.

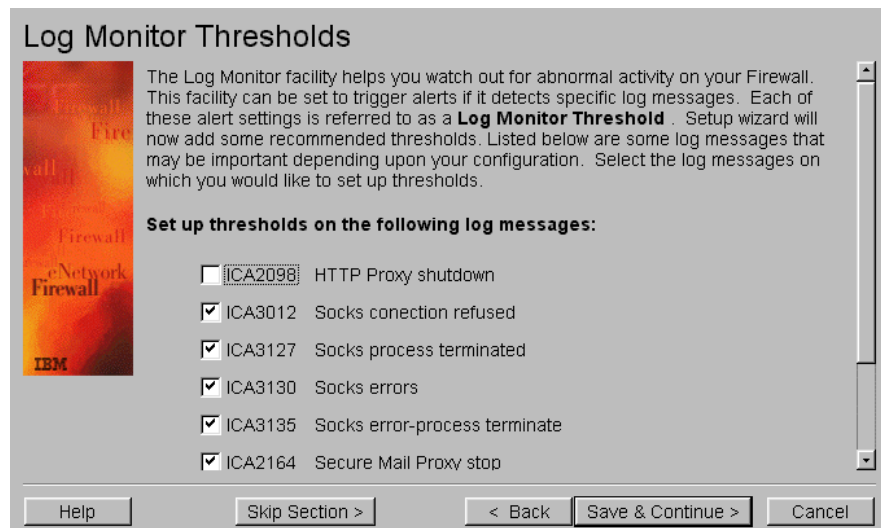


Figure 214. Log Monitor Thresholds

28. Select the thresholds. Click **Save & Continue**. The window shown in Figure 215 on page 166 appears.

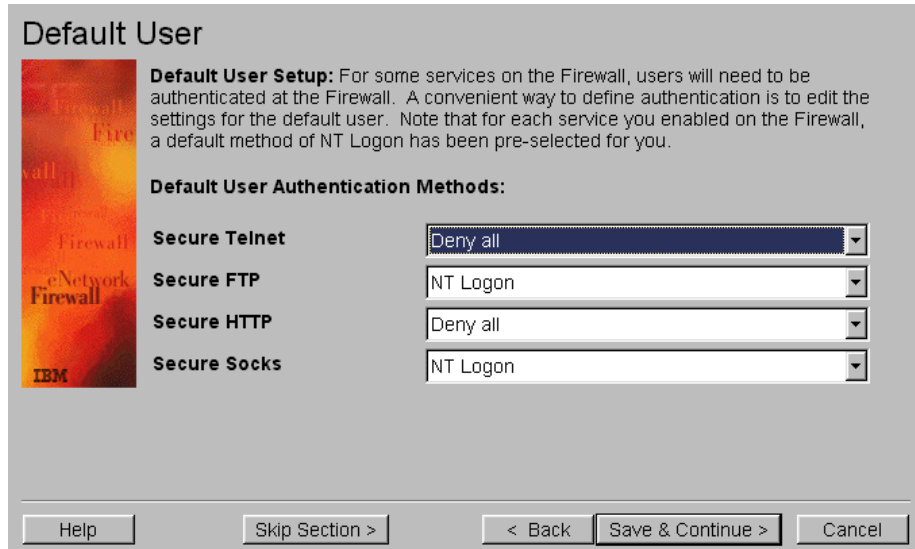


Figure 215. Default User Setup

29. For some services, a firewall user needs to be authenticated. Click **Save & Continue**. The window shown in Figure 216 appears.



Figure 216. Setup Activation

30. You can choose to activate your configuration now or at a later time. Click **Finish**.

IBM eNetwork Firewall for Windows NT configuration is now ready. For more information about IBM eNetwork Firewall for Windows NT, refer to Appendix D, “Firewall concepts” on page 349.

5.5 Configuring the SMTP server on the AS/400 MAILSRV3

This section describes the tasks that you must perform to install and configure an SMTP server on MAILSRV3 to handle mail using a firewall.

5.5.1 Task summary

The following list summarizes the tasks used to implement the SMTP server on the AS/400 MAILSRV3:

1. Set up the SMTP attributes.
2. Verify the MAILSRV3 TCP/IP domain name information.
3. Handle the SMTP mail domain on the AS/400 MAILSRV3.
4. Add the firewall name to the host table entries.
5. Start the SMTP server.

5.5.2 Setting up SMTP attributes

To route mail for Internet users to the firewall, you *must* configure the SMTP attributes in the AS/400 system to point to the firewall as the mail router. Entering the firewall name in the Mail router field tells the SMTP server where to forward mail that it cannot deliver itself. Complete these steps:

1. On an AS/400 command line, type:

```
CHGSMTPA
```

Press **F4** then Page Down.
2. You *must* enter ***YES** in the Firewall field. This tells the SMTP server that it is located behind a firewall.
3. Enter the correct values as shown in Figure 217, and press Enter.

```
Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

User ID delimiter . . . . . '?'          *SAME, *DFT, ?, =, ., &, $...
Mail router . . . . . > fw3mail.domain.com
                               (fw3nt.domain.com for the NT firewall)

Coded character set identifier  00819      1-65533, *SAME, *DFT
Mapping tables:
  Outgoing EBCDIC/ASCII table . *CCSID     Name, *SAME, *CCSID, *DFT
  Library . . . . .                Name, *LIBL, *CURLIB

  Incoming ASCII/EBCDIC table . *CCSID     Name, *SAME, *CCSID, *DFT
  Library . . . . .                Name, *LIBL, *CURLIB
Firewall . . . . . > *YES          *YES, *NO, *SAME
Journal . . . . . *NO             *YES, *NO, *SAME
Process all mail through MSF . . *NO     *YES, *NO, *SAME
Percent routing character . . . *YES     *YES, *NO, *SAME
```

Figure 217. Change SMTP Attributes

5.5.3 Verifying the HOME400 TCP/IP domain name information

Enter the Change TCP/IP Domain (**CHGTCPDMN**) command. In the Host name search priority field, type ***LOCAL**. Searching priority ***LOCAL** causes the AS/400

system to look at the host table entries first, before querying the DNS. Figure 218 shows the configuration values in the `CHGTCPDMN` command (or `CFGTCP` option 12) screen.

```

Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name . . . . . MAILSRV3

Domain name . . . . . domain3.com

Host name search priority . . . *LOCAL      *REMOTE, *LOCAL, *SAME

Internet address . . . . . 10.100.1.7

```

Figure 218. `CHGTCPDMN` - Search Priority `*LOCAL`

5.5.4 Handling the SMTP mail domain on the AS/400 MAILSRV3

The objective of this section is to set up the AS/400 system so MFS recognizes that it is listening for the SMTP domain name. You *must* add one IP address and add one host table entry for the mail domain name.

Follow this procedure on your AS/400 system:

1. On a command line, type `CFGTCP`. Press Enter.
2. Enter option 1 to add your TCP/IP address.
3. Enter option 10 to add one host table entry.
4. Associate the IP address with the mail domain in the host table entries.

Your host table should appear as shown in Figure 219.

```

Work with TCP/IP Host Table Entries
System: HOME400

Type options, press Enter.
 1=Add  2=Change  4=Remove  5=Display  7=Rename

Internet      Host
Opt  Address  Name

10.100.1.5    domain3.com
127.0.0.1     LOOPBACK
              LOCALHOST

```

Figure 219. Associating an IP address with the mail domain

The IP interface does not have to be started. It is only needed because the SMTP server looks on the host table to see which domain name is handled by the AS/400 IP address.

This IP address can also be virtual IP. See Appendix B, “Using virtual IP addresses” on page 329, for further information about this subject.

Tip

To verify that the AS/400 system is listening for a mail domain on a specific IP address, type `netstat *ifc` on a command line. Then, type `s` in front of the IP addresses you defined. The first line shows the domain associated with the interface.

5.5.5 Adding the firewall name to the host table entries

For the SMTP server to resolve the mail router name defined in the SMTP attributes (Figure 217 on page 167), you *must* configure one host table entry for the firewall.

Specify the internal secure IP address. Refer to Figure 187 on page 149 (interface B) for IBM Firewall for AS/400. Refer to Figure 193 on page 154 (interface B) for IBM eNetwork Firewall for Windows NT.

Figure 220 shows the TCP/IP host table configuration (CFGTCP option 10).

```
Work with TCP/IP Host Table Entries
System: MAILSRV3
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  7=Rename

  Internet      Host
  Opt  Address   Name
-----
      10.100.1.2  fw3mail
                          fw3mail.domain.com

(If you use the Windows NT firewall put this entry instead)
      10.100.1.2  fw3nt
                          fw3nt.domain.com
```

Figure 220. Firewall configuration on AS/400 TCP/IP host table

5.5.6 Starting the SMTP server

To start the SMTP server, complete these tasks:

1. Start the SMTP server using the command:

```
STRTCPSVR SERVER(*SMTP)
```

2. Verify that the Mail Server Framework (MSF) is running.

Use the `WRKACTJOB` command to determine if the mail server framework is running. Look in subsystem QSYSWRK for jobs named QMSF. If the QMSF job is not running, use the Start Mail Server Framework (`STRMSF`) command to start it.

The configuration of the SMTP server is now ready.

5.6 Configuring the POP3 server on the AS/400 MAILSRV3

This section describes the tasks that you must perform to install and configure a POP3 server on the AS/400 MAILSRV3. The POP server is a simple

store-and-forward mail system. It provides electronic mailboxes on the AS/400 system, from which clients can retrieve mail. It uses the AnyMail/400 mail server framework and the system distribution directory to process and distribute e-mail. It uses simple mail transfer protocol (SMTP) to forward mail.

5.6.1 Task summary

The following list summarizes the tasks used to implement the POP3 server on an AS/400 system:

1. Set the POP3 server attributes.
2. Add the POP3 user accounts.
3. Configure the POP3 accounts.
4. Start the POP3 server.

5.6.2 Setting up the POP3 server attributes

Complete these tasks to set up the POP3 server attributes:

1. On an AS/400 command line, type:

```
CHGPOPA
```
2. Press **F4**.
3. You *must* enter ***YES** in the Allow standard POP3 connection field. This tells the POP3 server that you are using a standard POP (TCP/IP) connection. We recommend setting the Message split size to ***NOMAX**.
4. Enter the correct values as shown in Figure 221, and press Enter.

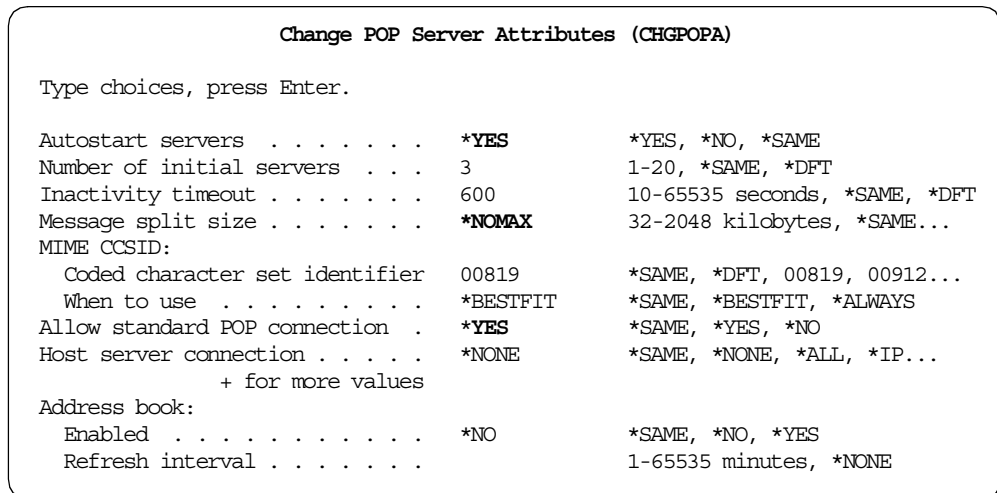


Figure 221. Change POP Server Attributes

5.6.3 Adding POP3 accounts

If your POP3 users are already AS/400 users, skip to 5.6.4, “Configuring POP3 accounts” on page 171. Complete these steps:

1. To create a new user profile on an AS/400 command line, type:

```
CRTUSRPRF
```

2. Press **F4**.

For security reasons, you may use the INLMNU (*SIGNOFF) parameter. This means that the user is not allowed to sign on to the AS/400 system.

3. Enter the correct values for the user. Use the example shown in Figure 222 as a guide. After you enter the correct values, press Enter.

```

Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . Estelle      Name
User password . . . . . *****  Name, *USRPRF, *NONE
Set password to expired . . . . *NO      *NO, *YES
Status . . . . . *ENABLED      *ENABLED, *DISABLED
User class . . . . . *USER        *USER, *SYSOPR, *PGMR...
Assistance level . . . . . *SYSVAL   *SYSVAL, *BASIC, *INTERMED...
Current library . . . . . *CRIDFT     Name, *CRIDFT
Initial program to call . . . . *NONE     Name, *NONE
  Library . . . . .           Name, *LIBL, *CURLIB
Initial menu . . . . . *SIGNOFF    Name, *SIGNOFF
  Library . . . . . *LIBL       Name, *LIBL, *CURLIB
Limit capabilities . . . . . *NO       *NO, *PARTIAL, *YES
Text 'description' . . . . . 'Estelle Jenni - POP3 account'

```

Figure 222. Creating a POP3 account

5.6.4 Configuring POP3 accounts

The way to configure a POP3 account on an AS/400 system is to add an entry in the system distribution directory for each user. For users who do *not* have a directory entry, follow these steps:

1. On an AS/400 command line, type:

```
WRKDIRE
```

Press Enter. the display shown in Figure 223 appears.

```

Work with Directory Entries

Type options, press Enter.
1=Add      2=Change  4=Remove  5=Display details  6=Print details
7=Rename   8=Assign different ID to description  9=Add another description

Opt  User ID  Address  Description
1
  *ANY      MAILSRV3  Generic entry for MAILSRV3
  DHQB      MAILSRV3  operations userid
  FSTEELE   MAILSRV3  Fant Steele
  QDFTOWN   QDFTOWN   Default Owner
  QDOC      QDOC      Internal Document Owner
  QLPAUTO   QLPAUTO   Licensed Program Automatic User
  QLPINSTL  QLPINSTL  Licensed Program Install
  QNOTES    QNOTES    LOTUS NOTES INTEGRATION PROFILE
  QSECOFR   QSECOFR   Security Officer

```

Figure 223. Work with Directory Entries

2. Type 1 and then press Enter. The display shown in Figure 224 on page 172 appears. In this document, we include only the relevant parameters in Figure 224 and Figure 225 and Figure 226 on page 172.

```

                                Add Directory Entry

Type choices, press Enter.

User ID/Address . . . . . ESTELLE  MAILSRV3
Description . . . . . Estelle Jermi - POP3 Account
System name/Group . . . MAILSRV3          F4 for list
User profile . . . . . ESTELLE          F4 for list
Network user ID . . . . .

```

Figure 224. Add Directory Entry (Part 1 of 2)

3. Press the Page Down key three times, or until you arrive at the display shown in Figure 225.

```

                                Add Directory Entry

Type choices, press Enter.

Mail service level . . . 2

                                1=User index
                                2=System message store
                                4=Lotus Domino
                                9=Other mail service

For choice 9=Other mail service:
Field name . . . . . F4 for list

Preferred address . . . 3

                                1=User ID/Address
                                2=O/R name
                                3=SMTP name
                                9=Other preferred address
                                F4 for list

Address type . . . . .
For choice 9=Other preferred address:
Field name . . . . . F4 for list

```

Figure 225. Add Directory Entry (Part 2 of 2)

4. Enter the values shown in Figure 225. Press **F19** (Add name for SMTP). The display shown in Figure 226 appears.

```

                                Add Name for SMTP
                                System:  MAILSRV3

Type choices, press Enter.

User ID . . . . . : ESTELLE
Address . . . . . : MAILSRV3

SMTP user ID . . . . . estelle
SMTP domain . . . . . domain3.com

SMTP route . . . . .

```

Figure 226. Adding an SMTP user ID and domain

5. Fill in the SMTP user ID and SMTP domain fields. These values are combined to form the SMTP e-mail address for this user (estelle@domain3.com). Press Enter.
6. To confirm your choice, press Enter again.

For users who *have* a directory entry, follow these steps:

1. On an AS/400 command line, type:

```
WRKDIRE
```

Press Enter. The display shown in Figure 227 appears.

```

                                Work with Directory Entries

Type options, press Enter.
  1=Add      2=Change  4=Remove  5=Display details  6=Print details
  7=Rename   8=Assign different ID to description  9=Add another description

Opt  User ID  Address  Description
-----
      *ANY    MAILSRV3  Generic entry for MAILSRV3
      DHQB   MAILSRV3  operations userid
      FSTEELE MAILSRV3  Fant Steele
  2   ESTELLE MAILSRV3  Estelle Jenni - POP3 Account
      QDFTOWN QDFTOWN  Default Owner
      QDOC    QDOC     Internal Document Owner
      QLPAUTO QLPAUTO  Licensed Program Automatic User
      QLPINSTL QLPINSTL Licensed Program Install

```

Figure 227. Work with Directory Entries

2. Type 2 beside the user's directory entry, and press Enter. The display shown in Figure 228 appears. In this redbook, we include only the relevant parameters in Figure 228 and Figure 229 on page 174.

```

                                Change Directory Entry

User ID/Address . . . . . : ESTELLE  MAILSRV3

Type changes, press Enter.

Description . . . . .    Estelle Jenni - POP3 account
System name/Group . . . MAILSRV3          F4 for list
User profile . . . . .  ESTELLE           F4 for list
Network user ID . . . . ESTELLE  MAILSRV3

                                                                More...
```

Figure 228. Change Directory Entry (Part 1 of 2)

3. Press the Page Down key four times or until you arrive at the display shown in Figure 229 on page 174.

```

Change Directory Entry

User ID/Address . . . . : ESTELLE   MAILSRV3

Type changes, press Enter.

Mail service level . . 2
                        1=User index
                        2=System message store
                        4=Lotus Domino
                        9=Other mail service

For choice 9=Other mail service:
Field name . . . . . F4 for list

Preferred address . . . 3
                        1=User ID/Address
                        2=O/R name
                        3=SMTP name
                        9=Other preferred address
                        F4 for list

Address type . . . . .
For choice 9=Other preferred address:
Field name . . . . . F4 for list
More...

```

Figure 229. Changing Directory Entry (Part 2 of 2)

4. Enter the values shown in Figure 229. Press **F19** (Add name for SMTP). The display shown in Figure 230 appears.

```

Change Name for SMTP
System: MAILSRV3

User ID/Address . . . . . : ESTELLE   MAILSRV3

Type choices, press Enter.

SMTP user ID . . . . . estelle
SMTP domain . . . . . domain3.com

SMTP route . . . . .

```

Figure 230. Adding an SMTP user ID and domain

5. Fill in the SMTP user ID and SMTP domain fields. These values are combined to form the SMTP e-mail address for this user (estelle@domain3.com). Press Enter.
6. To confirm your choice, press Enter again.

5.6.5 POP3 mailboxes

Once there is an entry in the system distribution directory for a POP mail user, the mailbox for that user is created automatically. This happens either the first time the client logs on successfully or when mail is received for the client.

5.6.6 Starting the POP3 server

To start the POP3 server, perform the following steps:

1. Start the POP3 server using the command:

```
STRTCPSVR SERVER(*POP)
```

2. Verify that the MSF (Mail Server Framework) is running.

Use the `WRKACTJOB` command to determine if the mail server framework is running (look in subsystem QSYSWRK for jobs named QMSF). If the QMSF job is not running, use the Start Mail Server Framework (`STRMSF`) command to start it.

The configuration of the POP3 server is now ready.

5.7 Planning the Domino server on AS/400 systems

This section describes the tasks that you must perform to plan Domino servers on AS/400 systems.

5.7.1 Planning considerations

There are several ways to implement a Domino server on an AS/400 system to handle SMTP mail:

- SMTP server on the Domino server
- SMTP server with MSF on the AS/400 system
- SMTP server with MSF on the AS/400 system and on the Domino server

The first configuration, SMTP server on the Domino server, is the one we implement in this scenario on the HOME400 system.

The second configuration, SMTP server with MSF on the AS/400 system, is documented in 5.9, “Configuring Domino with MSF on the AS/400 system” on page 183. This is implemented on the MAILSRV2 system.

The third possibility needs specific configurations. If you need to use both the SMTP server on the AS/400 system and the SMTP server on the Domino server, you have to bind each application to a specific IP address. Refer to the Dual Stack PTF cover letter. In V4R2, this is supported by PTF SF55697. In V4R3, this is supported by PTF SF58661. A PTF is under development for V4R4. These PTFs are OS/400 PTFs that are used to add the feature. The cover letter for the PTF also lists a corresponding co-requisite PTF from the POP snap-ins.

Table 22 on page 176 shows the configuration values for DOM400 and DOMINO2.

Table 22. Configuration values for DOM400 and DOMINO2

Values	DOM400	DOMINO2
AS/400	HOME400	MAILSRV2
Domino IP address	10.100.1.8	10.100.1.10
Host name	dom400	domino2
Domain name	domain.com	domain2.com
Server name	DOM400/DOMAIN	DOMINO2/DOMAIN2
Organization name	DOMAIN	DOMAIN2
Domino Domain	*ORG	*ORG
AS/400 Data directory	/domino/dom400/data	/domino/domino2/data
Internet packages	*SMTP	*SMTP
SMTP services	*DOMINO	*MSF
User.id	admin_dom400	admin_domino2
Cert.id	domain.id	domain2.id

Use Table 23 to record the configuration values that you will use to configure your systems.

Table 23. User configuration values

Values	DOM400	DOMINO2
AS/400		
Domino IP address		
Host name		
Domain name		
Server name		
Organization name		
Domino Domain		
AS/400 Data directory		
Internet packages		
SMTP services	*DOMINO	*MSF
User.id		
Cert.id		

5.8 Configuring the Domino server for mail

The task you must perform to set up the Domino server for this part of the scenario is similar to the task documented in 3.7, “Configuring the Domino server for mail” on page 71. In this section, we refer you to that procedure and only document the steps that are different for this scenario.

Refer to Table 22 on page 176 for the configuration values that you must use for these procedures.

5.8.1 Task summary

The following list summarizes the tasks used to implement the Domino server on the AS/400 HOME400:

1. Set up HOME400 to handle Domino.
2. Install the Domino server on HOME400.
3. Install Domino Administrator on your workstation.
4. Set up your workstation to administer Domino.
5. Configure the Domino server for SMTP mail.
6. Link the Domino server with the firewall.
7. Create Lotus Notes mail users.

Perform procedures 3.7.3, “Setting up HOME400 to handle Domino” on page 72, through 3.7.6, “Setting up your workstation to administer Domino” on page 78. This will guide you from task 1 through task 4 from the task list above. Return here when you reach “Stop here” on page 82.

5.8.2 Configuring Domino server for SMTP mail

This section describes how to set up the Domino server to handle SMTP mail. Refer to Table 22 on page 176 for the configuration values. Use the values in the column labeled DOM400.

On the Domino Administrator desktop, complete the following steps. Use the example in Figure 231 as a guide for the first five steps.

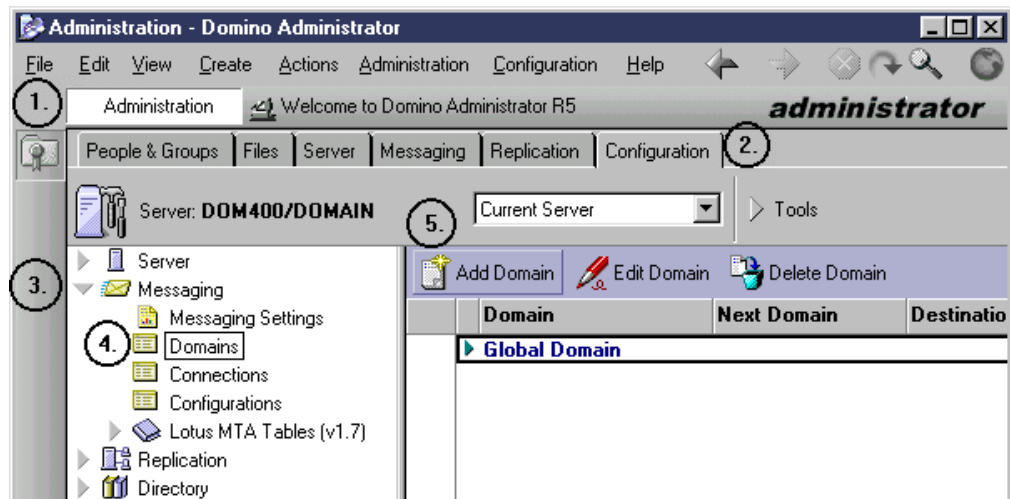


Figure 231. Domain document

1. Click the **Administration** button (1).
2. Click the **Configuration** tab (2).
3. Open **Messaging** in the navigation tree (3).
4. Click **Domains** (4).
5. Click the **Add Domain** button (5). The display shown in Figure 232 on page 178 appears.

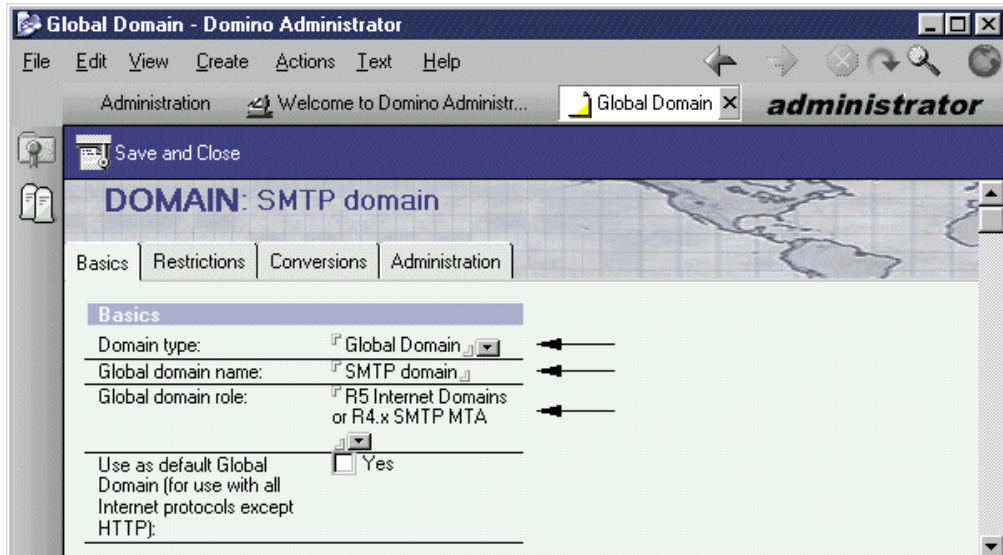


Figure 232. Domain document - Basics

6. Select **Global Domain** for Domain type.
7. Enter SMTP Domain for Global domain name.
8. Select **R5 Internet Domains** for Global domain role.
9. Click on the **Conversions** tab. The display shown in Figure 233 appears.

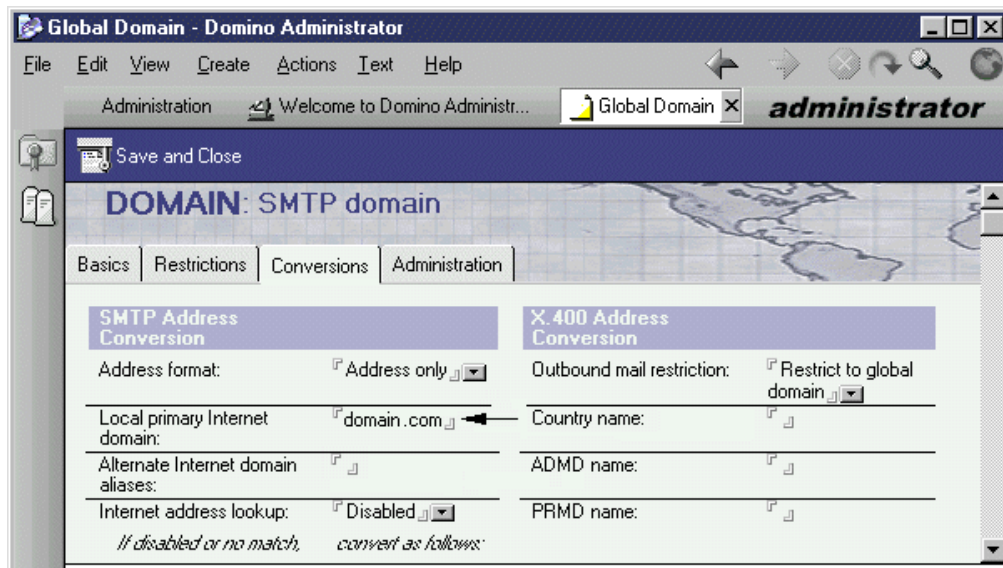


Figure 233. Domain document - Conversions

10. Enter domain.com for Local primary Internet domain.
11. Leave the Alternate Internet domain aliases field blank.
12. Click **Save and Close**. You return to a window similar to the window shown in Figure 231 on page 177.

Use Figure 234 on page 179 as a guide for the next three steps.

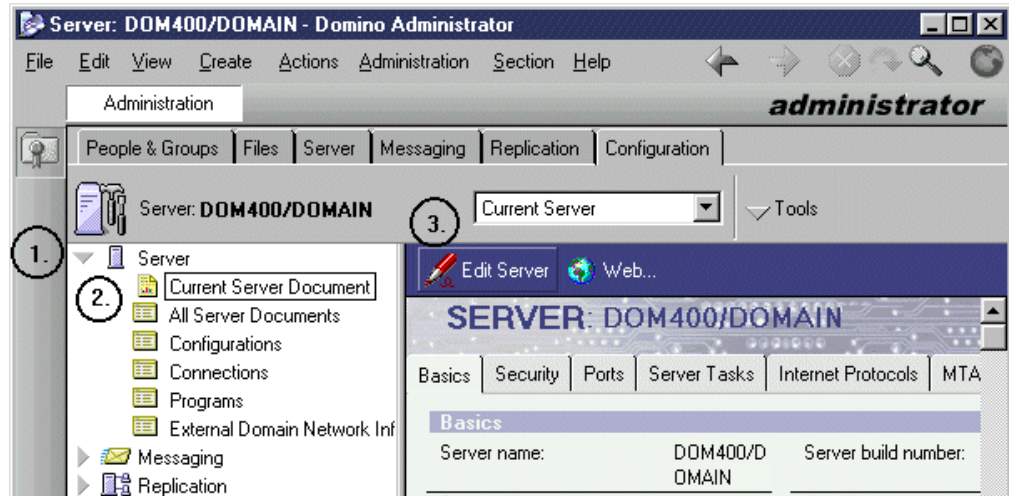


Figure 234. Server document

13. Open **Server** in the navigation tree (1).
14. Select **Current Server Document** (2).
15. Click the **Edit Server** button (3). The display shown in Figure 235 appears.

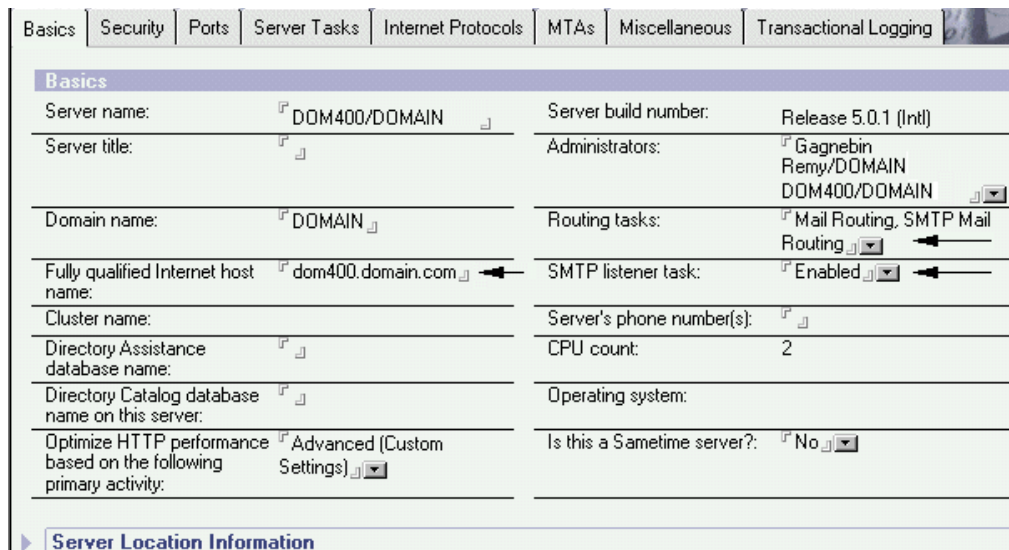


Figure 235. Server document - Basics

16. The Fully qualified Internet host name *must* match the Domino server name.
17. Verify that the SMTP listener task is `Enabled`.
18. Verify that the Routing tasks are `Mail Routing` and `SMTP Mail Routing`.
19. Click **Save and Close**.

You have now configured the Domino server to handle Internet mail using SMTP on the Domino server.

5.8.3 Linking the Domino server with the firewall

To link the Domino SMTP server with the firewall, complete the following steps. Use the example shown in Figure 236 as a guide for the first three steps.

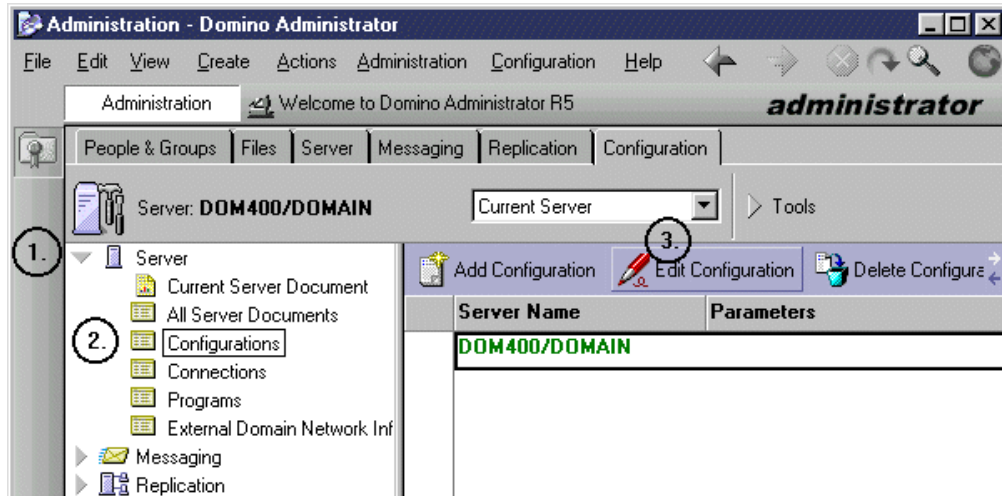


Figure 236. Configuration document

1. Open **Server** in the navigation tree (1).
2. Select **Configurations** (2).
3. Click the **Edit Configurations** button (3). The display shown in Figure 237 appears.

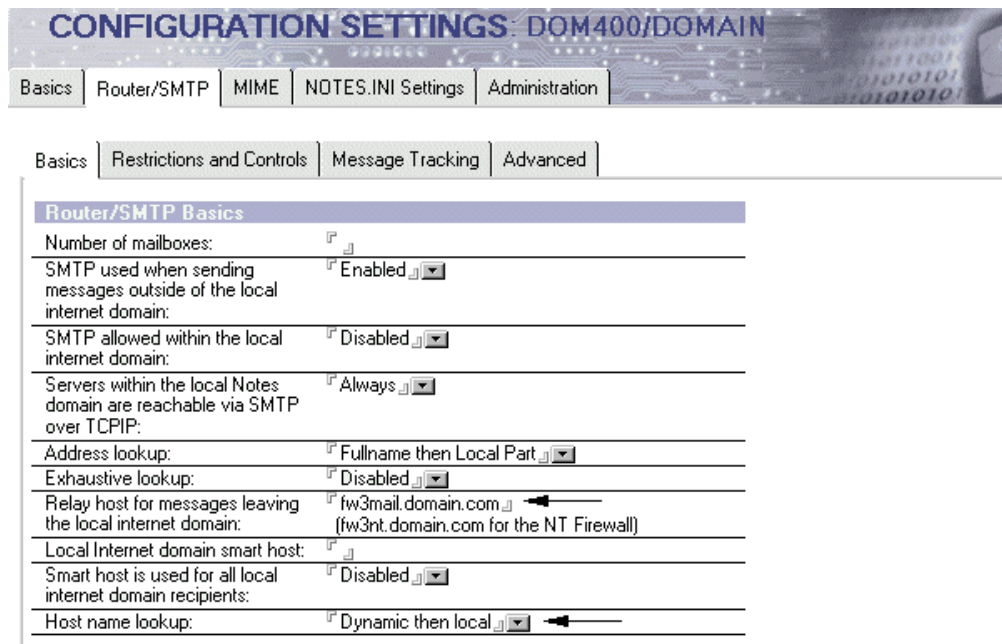


Figure 237. Configuration document - Router/SMTP

4. Click the **Router/SMTP** tab.
5. Enter the firewall name for Relay host for messages leaving the local Internet domain.

6. Verify that the Host name lookup is set to *Dynamic* then *local*.
7. Click **Save and Close**.

You have now linked the Domino SMTP server with the SMTP relay function of your firewall.

5.8.4 Creating Lotus Notes mail users

The Domino server is now ready to receive mail from the Internet. In this section we create a Lotus Domino user and their mailbox. To build the user and mailbox, perform the following steps. Use the example shown in Figure 238 as a guide for the first five steps.

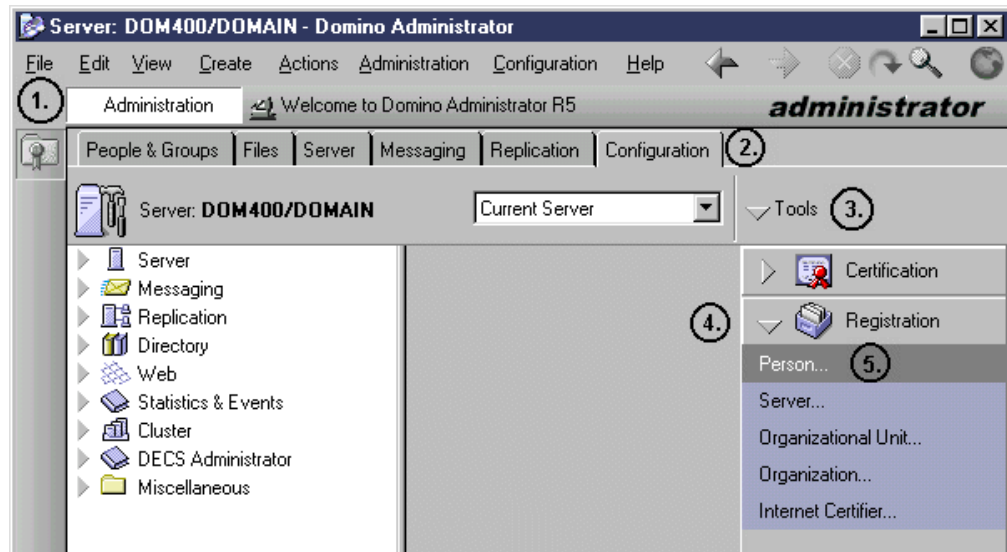


Figure 238. Registration - Person

1. On the Domino Administrator desktop, click **Administration** (1).
2. Click the **Configuration** tab (2).
3. Click the **Tools** pull-down menu (3).
4. Click **Registration** (4).
5. Click **Person** (5). The display shown in Figure 239 appears.



Figure 239. Certifier ID password

6. Enter the password, and then click **OK**.

Use the display shown in Figure 240 on page 182 to complete the next three steps.

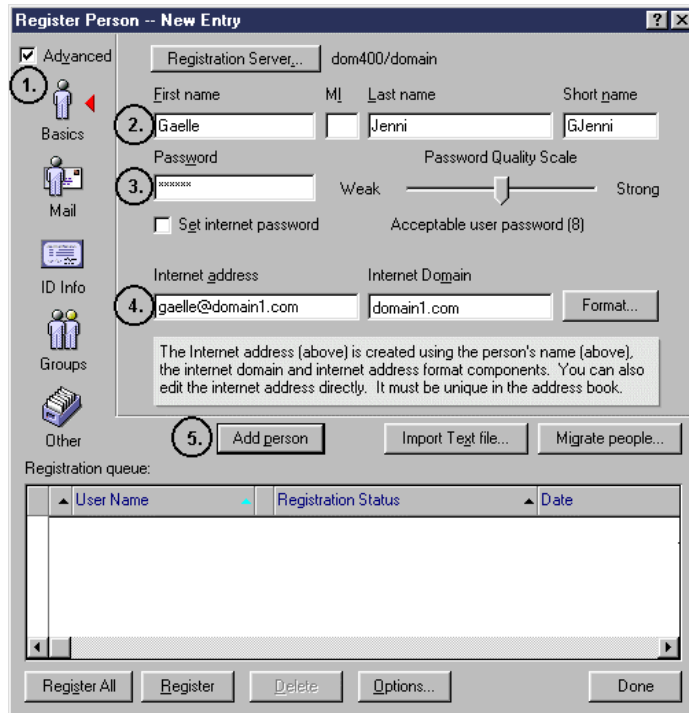


Figure 240. Register Person (Part 1 of 2)

7. Check **Advanced** (1).
8. Enter the person's first name and last name (2).
9. Enter the person's password (3).
10. Enter the person's Internet address and Internet domain (4).
11. Click the **Add person** button (5). The display shown in Figure 241 on page 183 appears.

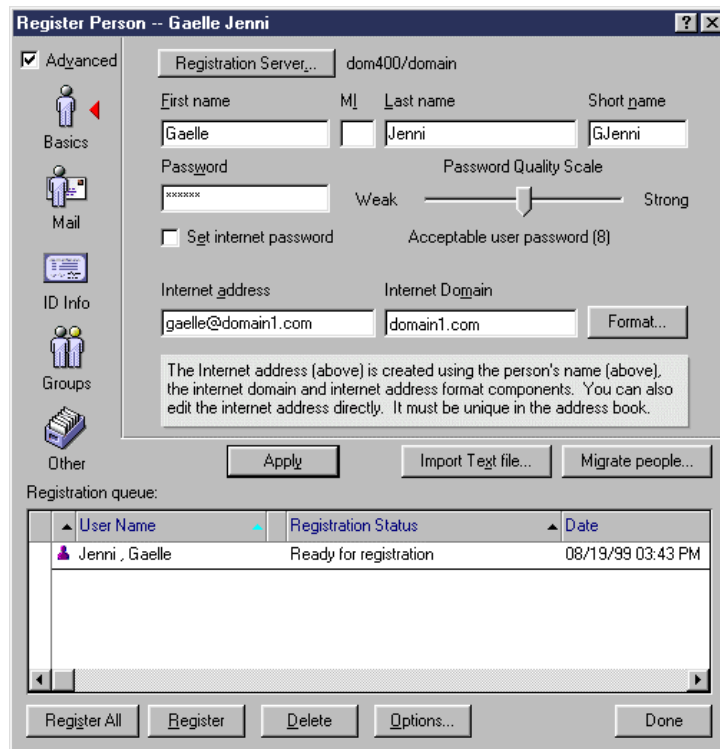


Figure 241. Register Person (Part 2 of 2)

12. Click the **Register** button.

The registration process can take several minutes.

You have now successfully registered your user and mailbox. The user ID is stored on the Domain's Public Address Book.

The last step is to configure Lotus Notes on your PCs. If you never before configured Lotus Notes for your mail, refer to the Lotus documentation that came with the product.

5.9 Configuring Domino with MSF on the AS/400 system

This section describes the tasks that you must perform to configure a Domino server with Mail Server Framework (MSF) on the AS/400 system to handle mail using a firewall. See 5.9.4, "Handling the SMTP domain using MSF on the AS/400 system" on page 185, for additional information.

5.9.1 Task summary

The following list summarizes the tasks used to implement the Domino server on the AS/400 HOME400:

1. Set up the SMTP attributes on MAILSRV2.
2. Verify the MAILSRV2 TCP/IP domain name information.
3. Handle the SMTP domain using SMTP on the AS/400 system.
4. Add the firewall name to the host table entries.
5. Start the MAILSRV2 SMTP server.

6. Set up MAILSRV2 to handle Domino.
7. Install the Domino server on MAILSRV2.
8. Set up your workstation to administer Domino.
9. Configure the Domino server for SMTP mail.
10. Link the Domino server with the firewall.
11. Create Lotus Notes mail users.

5.9.2 Setting up SMTP attributes on MAILSRV2

To route mail for Internet users to the firewall, you *must* configure the SMTP attributes in the AS/400 system to point to the firewall as the mail router. Entering the firewall name in the Mail router field tells the SMTP server where to forward mail that it cannot deliver itself. Complete these steps:

1. On an AS/400 command line, type:


```
CHGSMTPA
```
2. Press **F4**, and then press Page Down.
3. You *must* enter ***YES** in the Firewall field. This tells the SMTP server that it is located behind a firewall.
4. Enter the correct values as shown in Figure 242, and press Enter.

```

Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

User ID delimiter . . . . . '?'          *SAME, *DFT, ?, =, ., &, $...
Mail router . . . . . > fw3mail.domain.com
                               (fw3nt.domain.com for the NT firewall)

Coded character set identifier    00819      1-65533, *SAME, *DFT
Mapping tables:
  Outgoing EBCDIC/ASCII table .  *CCSID   Name, *SAME, *CCSID, *DFT
  Library . . . . .                Name, *LIBL, *CURLIB

  Incoming ASCII/EBCDIC table .  *CCSID   Name, *SAME, *CCSID, *DFT
  Library . . . . .                Name, *LIBL, *CURLIB
Firewall . . . . . > *YES          *YES, *NO, *SAME
Journal . . . . . *NO              *YES, *NO, *SAME
Process all mail through MSF . . *NO      *YES, *NO, *SAME
Percent routing character . . .  *YES     *YES, *NO, *SAME

```

Figure 242. Change SMTP Attributes

5.9.3 Verifying the MAILSRV2 TCP/IP domain name information

Enter the `CHGTCPDMN` command in the Host name search priority field. Type `*LOCAL`. Search priority `*LOCAL` causes the AS/400 system to look to the host table entries first, before querying the DNS.

Figure 243 on page 185 shows the configuration values in the `CHGTCPDMN` command (or `CFGTCP` option 12).


```

Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name . . . . . MAILSRV2

Domain name . . . . . domain2.com

Host name search priority . . . *LOCAL      *REMOTE, *LOCAL, *SAME

Internet address . . . . . 10.100.1.7

```

Figure 243. CHGTCPDMN - Search Priority *LOCAL

5.9.4 Handling the SMTP domain using MSF on the AS/400 system

The objective of this section is to set up the AS/400 system so MFS recognizes that it is listening for the SMTP domain name specified. Refer to Table 22 on page 176 for the configuration values. Use the values in the column labeled DOMINO2. You *must* add one IP address and add one host table entry for the SMTP mail domain name.

Complete the following procedure on your AS/400 system:

1. On a command line, type `CFGTCP`. Press Enter.
2. Enter option 1 to add your TCP/IP address.
3. Enter option 10 to add one host table entry.
4. Associate the IP address with the mail domain on the host table entries.

Your host table should appear as shown in Figure 244.

```

Work with TCP/IP Host Table Entries
System: MAILSRV2

Type options, press Enter.
 1=Add  2=Change  4=Remove  5=Display  7=Rename

Internet      Host
Opt Address    Name

10.100.1.4    domain2.com
127.0.0.1     LOOPBACK
              LOCALHOST

```

Figure 244. Associating an IP address with a mail domain

The IP interface does not have to be started. It is only needed because the SMTP and MSF servers look in the host table to see which SMTP domain names are handled by this AS/400 system. If the SMTP domain name matches an IP address defined on the AS/400 system, then the mail is accepted and processed.

This IP address can also be a virtual IP address. See Appendix B, “Using virtual IP addresses” on page 329, for further information.

Tip

To verify that the AS/400 system is listening for a mail domain on a specific IP address, type `netstat *ifc` on a command line. Then, type `5` in front of the IP addresses that you defined. The first line shows the domain associated with the interface.

5.9.5 Adding the firewall name to the host table entries

For the SMTP server to resolve the mail router name defined in the SMTP attributes (Figure 242 on page 184), you *must* configure a host table entry for the firewall.

Specify the internal secure IP address. Refer to Figure 187 on page 149 (interface B) for the *IBM Firewall for AS/400* and Figure 193 on page 154 (interface B) for *IBM eNetwork Firewall for Windows NT*.

Figure 245 shows the TCP/IP host table configuration (CFGTCP option 10).

```
Work with TCP/IP Host Table Entries                               System:  MAILSRV2
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  7=Rename

  Internet      Host
  Opt  Address   Name

      10.100.1.2  fw3mail
                          fw3mail.domain.com

(If you use the Windows NT firewall put this entry instead)
      10.100.1.2  fw3nt
                          fw3nt.domain.com
```

Figure 245. Firewall configuration on the AS/400 TCP/IP host table

5.9.6 Starting the MAILSRV2 SMTP server

To start the SMTP server, complete these tasks:

1. Enter the command:

```
STRTCPSVR SERVER(*SMTP)
```

2. Verify that the MSF is running.

Use the `WRKACTJOB` command to determine if the mail server framework (MSF) is running. Look in subsystem `QSYSWRK` for jobs named `QMSF`. If the `QMSF` job is not running, use the Start Mail Server Framework (`STRMSF`) command to start it.

The configuration of the SMTP server is now ready.

5.9.7 Setting up MAILSRV2 to handle Domino

To use Domino on an AS/400 platform, we strongly recommend that you add a unique TCP/IP address for each Domino server. Follow these steps:

1. On an AS/400 command line, type `ADDTCPIFC F4`. The screen in Figure 246 appears.

```

                                Add TCP/IP Interface (ADDTCPIFC)

Type choices, press Enter.

Internet address . . . . . 10.100.1.10
Line description . . . . . TRNLINE      Name, *LOOPBACK...
Subnet mask . . . . . 255.255.255.0
Associated local interface . . . *NONE
Type of service . . . . . *NORMAL      *MINDELAY, *MAXTHRPUT...
Maximum transmission unit . . . *LIND      576-16388, *LIND
Autostart . . . . . *YES      *YES, *NO
PVC logical channel identifier
+ for more values
X.25 idle circuit timeout . . . 60      1-600
X.25 maximum virtual circuits . 64      0-64
X.25 DDN interface . . . . . *NO      *YES, *NO
TRNLAN bit sequencing . . . . . *MSB      *MSB, *LSB
```

Figure 246. Add TCP/IP Interface

2. Enter the IP address, line description, and subnet mask.
3. Press Enter.
4. Start the IP interface by typing `9` beside the IP address.

You have now added a TCP/IP interface to your AS/400 system. This IP address can also be a virtual IP address. See Appendix B, “Using virtual IP addresses” on page 329, for further information.

5.9.8 Installing the Domino server on MAILSRV2

Install the Domino server using the instructions in *Lotus Domino for AS/400 R5: Implementation*, SG24-5592. Refer to Table 22 on page 176 for the configuration values. Use the values in the column labeled DOMINO2.

If you do not have this redbook and do not have Internet access to download it, you can review the parameters shown in Figure 247 on page 188 to Figure 250 on page 189. Follow these steps:

1. Insert the CD-ROM Lotus Domino for AS/400.
2. Install the product using the command:

```
LODRUN DEV(*OPT) DIR('/OS400')
```

3. On an AS/400 command line, type: `CFGDOMSVR F4`

Note

In this configuration, we use the AS/400 Mail Server Framework (MSF) to receive the SMTP mail. The mail is processed by OS/400 TCP/IP MSF and SMTP before it is passed to the Domino server. The key parameter in the CFGDOMSVR command to make this work correctly is SMTP Services with a value of *MSF (not *DOMINO) as shown in Figure 248 on page 188.

```
Configure Domino Server (CFGDOMSVR)

Type choices, press Enter.

Server name . . . . . > DOMINO2

Option . . . . . > *FIRST          *FIRST, *ADD, *REMOVE
Data directory . . . . . > '/DOMINO/DOMINO2/DATA'

Organization . . . . . > DOMAIN2
```

Figure 247. Configure Domino Server (Part 1 of 4)

```
Configure Domino Server (CFGDOMSVR)

Type choices, press Enter.

Administrator:
Last name . . . . . > Remy

First name . . . . . > Gagnebin
Middle initial . . . . .
Password . . . . . > lartisan
Minimum password length . . . 8
Internet password . . . . . *NONE
Time zone . . . . . > CST
Daylight savings time . . . . . > *NO
Web browsers . . . . . > *NONE

Internet mail packages . . . . . > *SMTP
+ for more values
SMTP services . . . . . *MSF
```

Figure 248. Configure Domino Server (Part 2 of 4)

```

                                Configure Domino Server (CFGDOMSVR)

Type choices, press Enter.

Directory services . . . . . *NONE          *NONE, *ALL, *SYSDIR, *LDAP

News readers . . . . . *NONE             *NONE, *NNTP
Connection services . . . . . *DECS        *DECS, *NONE
Advanced services . . . . . *NONE          *NONE, *ALL, *PARTITION...
                                + for more values

                                Additional Parameters

Replace configuration . . . . . *YES         *YES, *NO
Domain name . . . . . *ORG
Network name . . . . . NETWORK1
Country code . . . . . > *BLANK
Certifier ID . . . . . *GEN

```

Figure 249. Configure Domino Server (Part 3 of 4)

```

                                Configure Domino Server (CFGDOMSVR)

Type choices, press Enter.

Administrator ID . . . . . *GEN

Server ID . . . . . *GEN

Start server . . . . . *YES               *YES, *NO
Log replication events . . . . . *YES      *YES, *NO
Log client session events . . . *YES       *YES, *NO
TCP/IP port options:
  Encrypt network data . . . . . *NOENCRYPT *ENCRYPT, *NOENCRYPT
  Internet address . . . . . > '10.100.1.10'
Subsystem and object names . . . *GEN     Name, *GEN
Collation . . . . . *STD                  *STD, CS, DA-DK-AA, DE, E2-ES ...
Copy Administrator ID file . . . *ALL     *DOMDIR, *DTADIR, *ALL
Additional services . . . . . *NONE        *NONE, *ICM
                                + for more values

```

Figure 250. Configure Domino Server (Part 4 of 4)

5.9.9 Setting up your workstation to administer the Domino server

Refer to 3.7.6, “Setting up your workstation to administer Domino” on page 78, to set up your workstation to administer the Domino server. Refer to Table 22 on page 176 for the configuration values. Use the values in the column labeled DOMINO2.

5.9.10 Configuring the Domino server for SMTP mail

Now, set up the Domino server to handle SMTP mail that is received by MSF on the AS/400 system. The main difference here is that we specify values in the MTAGlobal domain rather than create a new domain. Refer to Table 22 on page 176 for the configuration values.

On the Domino Administrator desktop, complete the following steps. Use the example in Figure 251 as a guide for the first six steps.

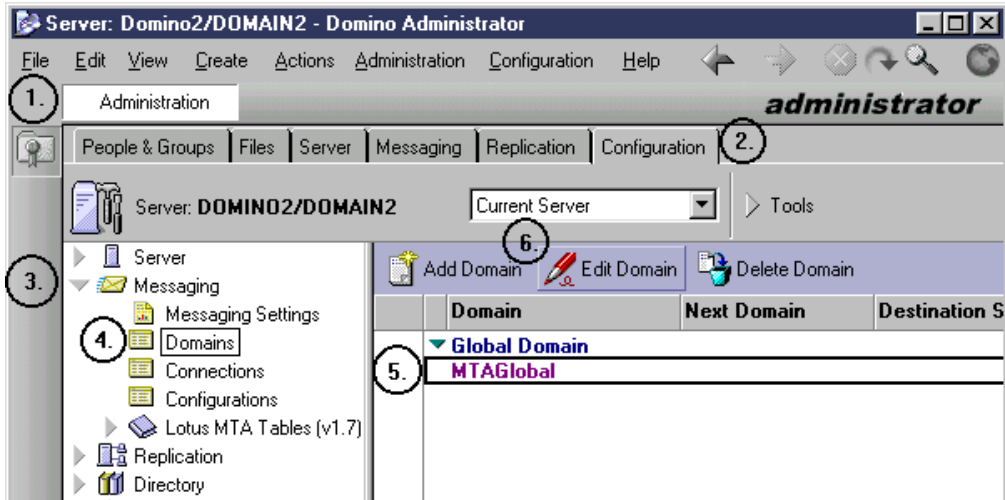


Figure 251. Domain document (MTAGlobal)

1. Click the **Administration** button (1).
2. Click the **Configuration** Tab (2).
3. Open **Messaging** in the navigation tree (3).
4. Click **Domains** (4).
5. Select the **MTAGlobal** domain (5).
6. Click the **Edit Domain** button (6). The display shown in Figure 252 appears.

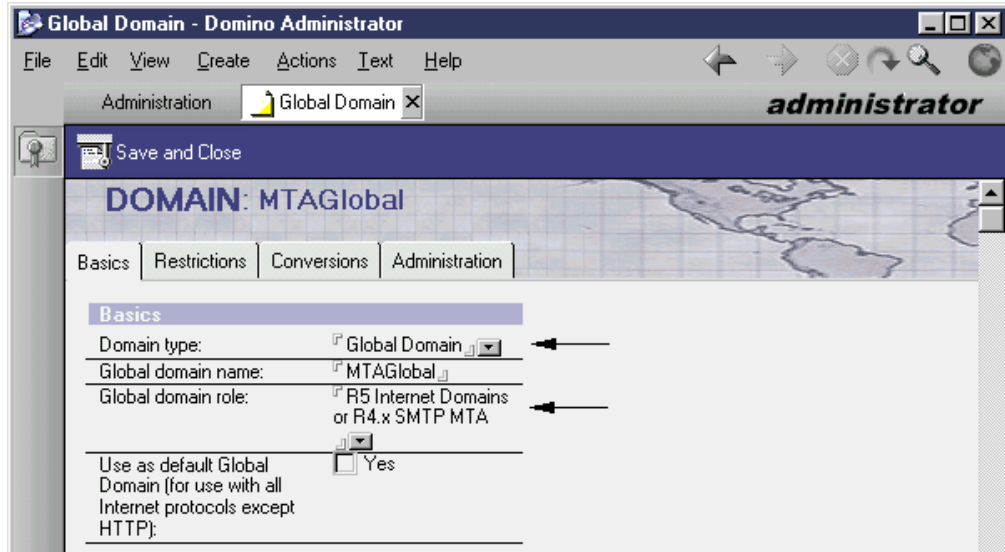


Figure 252. Domain document - Basics (MTAGlobal)

7. Verify that the Domain type is Global Domain.
8. Verify that the Global domain role is R5 Internet Domains.
9. Click on the **Conversions** tab. The display shown in Figure 253 appears.

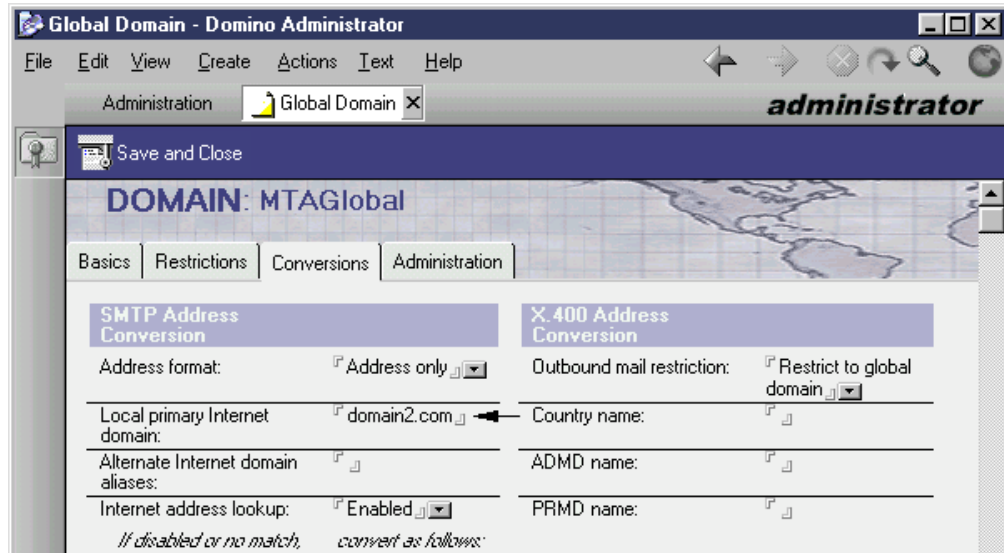


Figure 253. Domain document - Conversion (MTAGlobal)

10. Enter `domain2.com` for Local primary Internet domain.

11. Click **Save and Close**.

Refer to Figure 254 for steps 12 through 14.

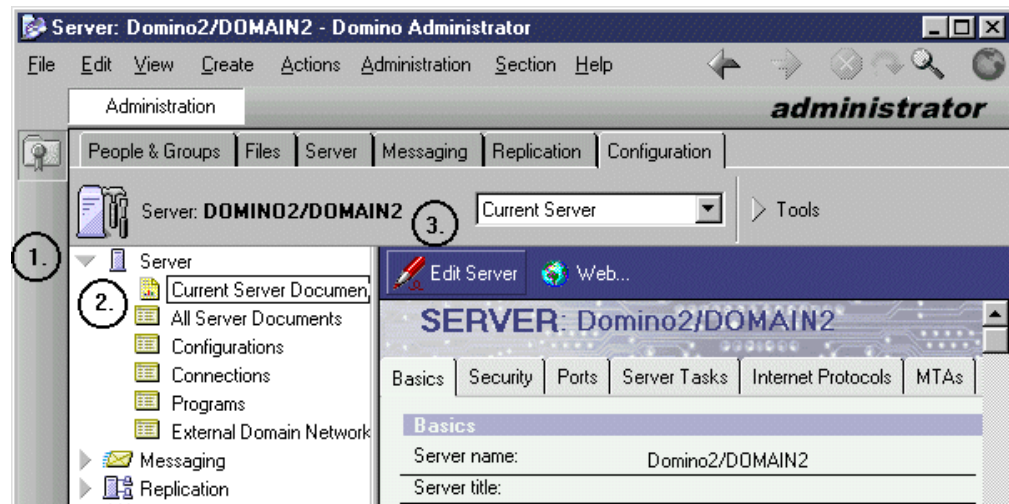


Figure 254. Server document

12. Open **Server** in the navigation tree (1).

13. Select **Current Server Document** (2).

14. Click the **Edit Server** button (3). The display shown in Figure 255 on page 192 appears.

Basics	Security	Ports	Server Tasks	Internet Protocols	MTAs	Miscellaneous	Transactional Logging
Basics							
Server name:	DOMINO2/DOMAIN2			Server build number:	Release 5.0.1 (Intl)		
Server title:				Administrators:	Gagnebin Remy/DOMAIN2 DOMINO2/DOMAIN2		
Domain name:	DOMAIN2			Routing tasks:	Mail Routing, SMTP Mail Routing		
Fully qualified Internet host name:	domino2.domain2.com			SMTP listener task:	Enabled		
Cluster name:				Server's phone number(s):			
Directory Assistance database name:				CPU count:	2		
Directory Catalog database name on this server:				Operating system:			
Optimize HTTP performance based on the following primary activity:	Advanced (Custom Settings)			Is this a Sametime server?:	No		

Figure 255. Server document - Basics

15. The Fully qualified Internet host name *must* match the Domino server name.

16. Verify that the SMTP listener task is Enabled.

17. Verify that the Routing tasks are Mail Routing and SMTP Mail Routing.

18. Click the **MTAs** tab. The display shown in Figure 256 appears.

Basics	Security	Ports	Server Tasks	Internet Protocols	MTAs	Miscellaneous	Transactional Logging	Administration
R4.x SMTP MTA X.400 MTA cc:Mail MTA								
R4.x Internet Message Transfer Agent (SMTP MTA) The following settings only apply to SMTP MTA versions 1.x and 4.x. To configure R5 SMTP Routing please refer to the Server's Server Configuration form.								
General					Control			
Global domain name:	MTAGlobal			Poll for new messages every:	120 seconds			
MTA administrator:				MTA work path:				
				Log level:	Normal			
				Enable daily housekeeping:	Enable			
				Perform daily housekeeping at:	01:00 AM			

Figure 256. Server document - MTAs

19. Verify that the Global domain is MTAGlobal.

20. Click **Save and Close**.

You have now configured the Domino server to handle Internet mail using SMTP and MSF on the AS/400 system.

5.9.11 Creating Lotus Notes mail users

Refer to 5.8.4, "Creating Lotus Notes mail users" on page 181, to set up your Lotus Notes user. Refer to Table 22 on page 176 for the configuration values.

Chapter 6. Single domain with a fanout to multiple systems

This chapter presents the procedures for configuring firewalls that support a single domain mail environment with multiple mail servers. It includes the procedures for setting up the configuration of both IBM Firewall for AS/400 and IBM eNetwork Firewall for Windows NT. The chapter also contains the procedures that we used to set up Domino servers on three AS/400 systems.

6.1 Scenario

In this scenario, we present a company that has one mail domain with multiple AS/400 systems each running a Domino server. The public mail domain and the private mail domain are the same.

The internal DNS can be on any AS/400 system on the network. In our scenario, the AS/400 HOME400 handles this function. The three mail servers are Domino servers using the SMTP support in Domino (not MSF). The firewall is either IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT

If you want to open the firewall to allow POP3 or Domino clients to access the internal mail server from the Internet, refer to 3.3.5, "Planning NAT to map the POP3 server address outside the firewall" on page 33, through 3.3.10, "Filter rules to allow Domino access from the Internet" on page 38, for IBM Firewall for AS/400. Refer to 3.4.5, "Planning NAT to map POP3 server address outside the firewall" on page 51, through 3.4.9, "Creating a service" on page 56, for IBM eNetwork Firewall for Windows NT.

6.1.1 Scenario network configuration

Figure 257 on page 194 illustrates a logical view of the network configuration used in this scenario. All the mail arrives at HOME400 and is then passed to the correct mail server.

There are three ways to implement the firewall:

- The firewall is an Integrated Netfinity Server running IBM Firewall for AS/400
- The firewall is a separate PC running Windows NT Server and IBM eNetwork Firewall for Windows NT,
- The firewall is an Integrated Netfinity Server running IBM eNetwork Firewall for Windows NT.

The procedure for setting up Windows NT Server on an Integrated Netfinity Server is provided in Chapter 8, "Installing a Windows NT Server to support firewalls" on page 289.

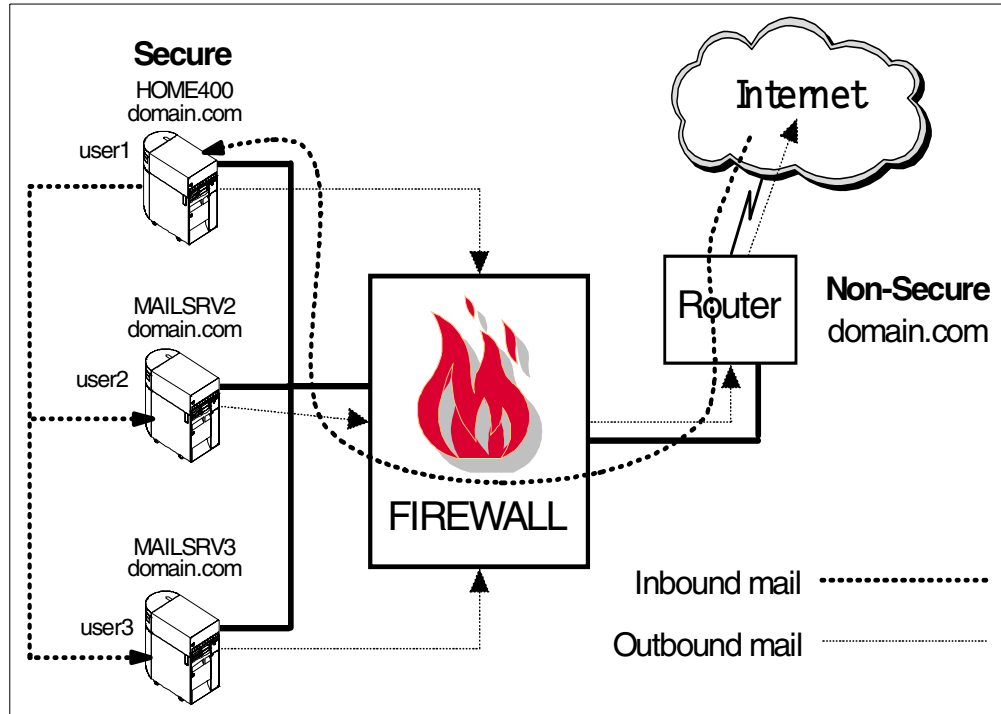


Figure 257. Scenario network configuration for one domain with fanout

6.1.2 Scenario objectives

The objectives of this scenario are:

- Configure the IP domain on the internal DNS.
- Configure the firewall so that it can handle the mail domain.
- Configure the HOME400 to handle Domino as a gateway between SMTP inbound (Internet) mail and NRPC (Lotus Notes) outbound mail.
- Configure the HOME400, MAILSRV2 and MAILSRV3 to handle NRPC (Lotus Notes) inbound and outbound mail.
- Configure the HOME400, MAILSRV2 and MAILSRV3 to handle SMTP outbound (Internet) mail.

6.1.3 Scenario advantages

This scenario has the following advantages:

- The firewall can be either IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT.
- IBM Firewall for AS/400 can handle the DNS function, so you do not need to spend extra money to handle this function by your ISP or on other DNS in the DMZ.
- Inbound SMTP mail is processed in one single Domino server. This is an opportunity to have an antivirus system scanning mail coming from the Internet.
- Outbound SMTP mail is processed on each Domino server, minimizing the chance of having a bottleneck in your Domino gateway.

6.1.4 Scenario limitations

There are also some limitations associated with this scenario. They include:

- The DNS function of IBM eNetwork Firewall for Windows NT uses the NT DNS in a cache-only mode. This means that a DNS is needed in the DMZ or you will have to use the DNS of your ISP (using the ISP DNS may mean extra fees).
- Inbound SMTP mail is processed on a single system. If you have heavy mail traffic it can create a bottleneck in your network.

6.1.5 Planning considerations

Consider the following points when planning to implement:

- Is there any internal DNS in your company?
- Are the PCs configured to handle an internal DNS?
- Are you using IBM Firewall for AS/400 or IBM eNetwork Firewall for Windows NT as your firewall?

The remainder of this chapter documents the procedures used to set up the firewall and mail server using both firewall products and both mail products. You should choose the sections that are appropriate for your environment.

- FW4MAIL refers to IBM Firewall for AS/400.
- FW4NT refers to IBM eNetwork Firewall for Windows NT.
- HOME400 refers to the first AS/400 system.
- MAILSRV2 refers to the second AS/400 system.
- MAILSRV3 refers to the third AS/400 system.
- DOM400 refers to the Domino server on AS/400 HOME400.
- DOMINO2 refers to the Domino server on AS/400 MAILSRV2.
- DOMINO3 refers to the Domino server on AS/400 MAILSRV3.

Table 24 lists the domains names, host names, and IP addresses used for this scenario.

Table 24. Domain names, host names, and IP addresses

Secure domain name	Host name	IP address
domain.com	fw4nt (non-secure)	208.222.150.250
domain.com	fw4nt	10.100.1.2
domain.com	fw4mail (non-secure)	208.222.150.250
domain.com	fw4mail	10.100.1.2
domain.com	fw4mail (internal LAN)	192.168.2.2
domain.com	home400	10.100.1.7
domain.com	home400 (internal LAN)	192.168.2.1

Secure domain name	Host name	IP address
domain.com	dom400	10.100.1.8
domain.com	mailsrv2	10.100.1.9
domain.com	domino2	10.100.1.10
domain.com	mailsrv3	10.100.1.11
domain.com	domino3	10.100.1.12
(Host table entry)	domain.com	10.100.1.3

Table 25 lists the values used to configure the AS/400 DNS for this scenario using different SMTP servers.

Table 25. Secure mail server name - DNS MX values

Firewall product	Secure domain name	MX value for mail server name for Domino SMTP
IBM Firewall for AS/400	domain.com	dom400.domain.com.
IBM eNetwork Firewall for Windows NT	domain.com	dom400.domain.com.

Table 26 lists the values used to configure the SMTP mail relay on the firewall for this scenario using the different firewall and mail products.

Table 26. Domain name and secure mail server name - firewall values

Firewall product	Secure and public domain name	Firewall mail server name for Domino SMTP
IBM Firewall for AS/400	domain.com	domain.com
IBM eNetwork Firewall for Windows NT	domain.com	dom400.domain.com

In Table 27, list the domain names, host names, and IP addresses you need for this scenario.

Table 27. User values for domain name, host name, and IP address

Domain name	Host name	IP address

Domain name	Host name	IP address
(Host table entry)		
(Host table entry)		
(Host table entry)		

In Table 28, list the values you need to configure the AS/400 DNS for this scenario.

Table 28. User values for the secure mail server name - DNS MX values

Firewall product	Secure domain name	MX value for mail server name for AS/400 SMTP	MX value for mail server name for Domino SMTP

In Table 29, list the values you need to configure the SMTP mail relay on the firewall for this scenario.

Table 29. User values for the domain name and secure mail server name - Firewall

Firewall product	Secure and public domain name	Firewall mail server name for AS/400 SMTP	Firewall mail server name for Domino SMTP

6.1.6 Task summary

To set up this scenario, you must configure the DNS to support the mail environment (step 1), configure a firewall (step 2 or 3), and configure your mail servers (steps 4 and 5). A summary of the procedure is listed here:

1. Configure the AS/400 DNS.
2. Configure IBM Firewall for AS/400 (FW4MAIL).
3. Configure IBM eNetwork Firewall for Windows NT (FW4NT).
4. Configure the three Domino servers.
5. Link the three Domino servers together.

6.2 Configuring the AS/400 DNS

This section describes the tasks that you must perform to configure the internal AS/400 DNS to handle the domain and mail servers. If the DNS is not already installed, refer to *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147.

6.2.1 Task summary

To configure the AS/400 DNS for this scenario, perform the following steps:

1. Configure the AS/400 DNS to handle the internal domain.
2. Add a host name to the domain.
3. Configure the MX record for each domain.
4. Configure the internal DNS to forward the queries to the firewall.

6.2.2 Configuring the AS/400 DNS to handle internal domain

To configure the AS/400 DNS, use Operations Navigator. It is included as part of Client Access Express for Windows.

To access the DNS configuration, select your **AS/400 system name** ->**Network**->**Server**->**TCP/IP**. Double-click **DNS**. Click the + symbol beside the DNS Server - Home400 (system name) entry. The window shown in Figure 258 is displayed.

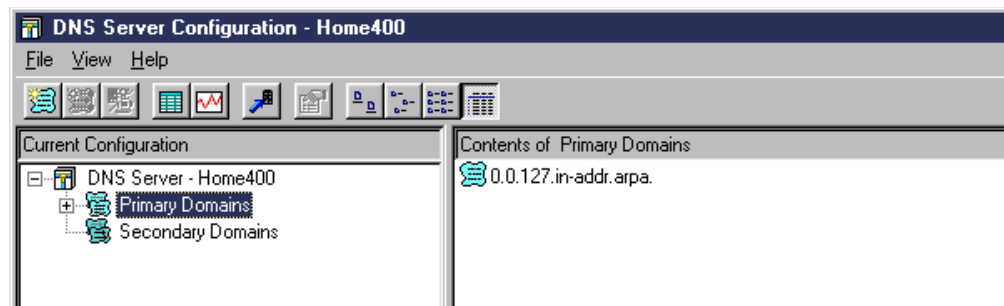


Figure 258. Configuring the AS/400 DNS to handle the internal domain domain.com

To add a primary domain, perform the following tasks.

1. Right-click on **Primary Domains**. Select **New Primary Domain**. The window shown in Figure 259 on page 199 is displayed.

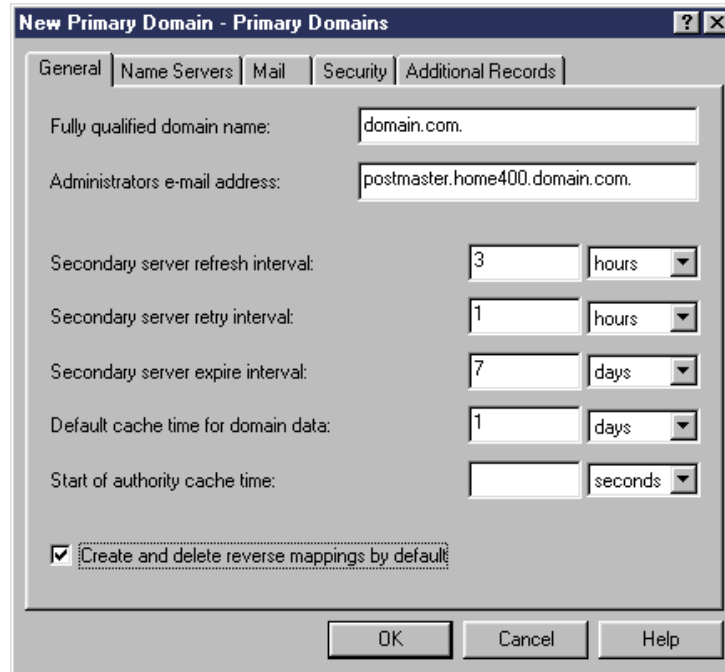


Figure 259. New Primary Domain domain.com

2. Enter the domain name `domain.com.` You *must* to put a dot at the end of your domain because it is a fully qualified domain name.
3. Check **Create and delete reverse mappings by default**.
4. Click **OK**. The window shown in Figure 260 is displayed. Your domain name is displayed in the right-hand frame.
5. Right-click on the domain name you added. A drop-down menu appears. Click **Enable**. This enables the domain in the DNS.

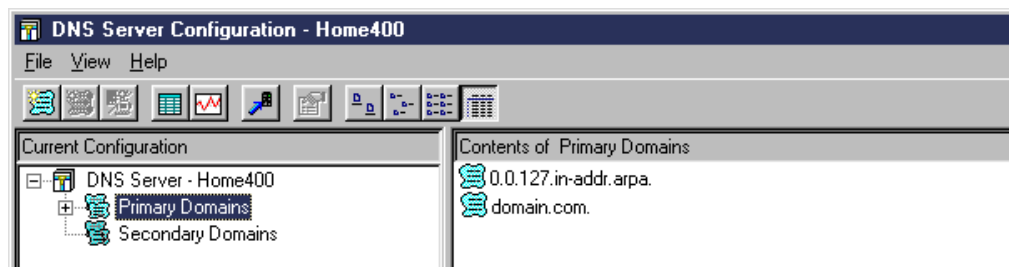


Figure 260. Contents of Primary Domains after creating domain.com

You have now successfully created your domain.

6.2.3 Adding host names to the domain

After creating the domains, you need to add the host name to the domain. Start from the window shown in Figure 260. To add the systems, perform the following steps:

1. Right-click **domain.com**.
2. Select **New Host**.

3. Click **Add**. The New Host window is displayed (Figure 261).

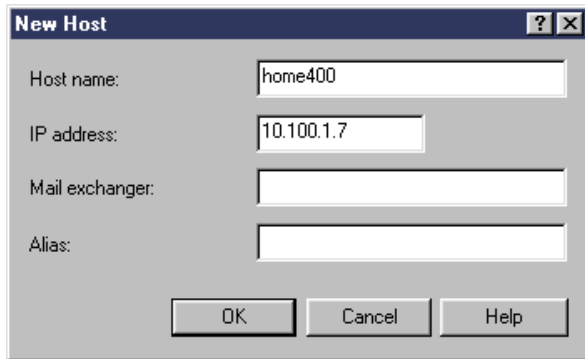


Figure 261. Adding the AS/400 host name

4. Enter the AS/400 host name and the IP address.

5. Click **OK**.

Repeat the steps in this section to add each host name of *domain.com* that is listed in Table 24 on page 195. Only the host names that have a 10.100.1.x IP address need to be stored in the DNS.

Now you need to add the mail exchange (MX) information for the mail domain.

6.2.4 Configuring the MX record for your domain

The MX record tells the DNS client (it can be either a PC or another DNS) the name of the SMTP server that processes mail for the domain. Start from the window shown in Figure 260 on page 199. To add the MX records, perform the following steps:

1. Right-click **domain.com**.
2. Select **Properties**.
3. Click the **Mail** tab.
4. Click **Add**. The window shown in Figure 262 is displayed.

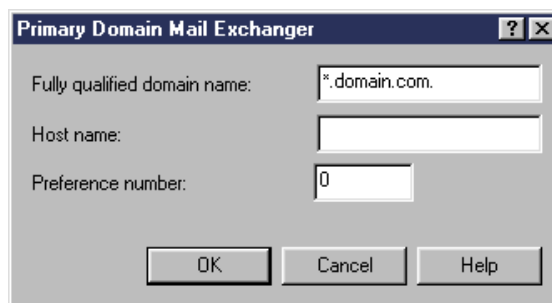


Figure 262. Adding an MX record in a domain

5. Remove the asterisk (*) from the front of the default domain name (*.domain.com.) to change it to domain.com. Change the preference number to 10.
6. Enter the host name of the SMTP server as dom400.

7. Click on **OK**.
8. Repeat steps 4 through 6 and add another MX record with a host name of `Domino2` and a preference number of 20.
9. Repeat steps 4 through 6 and add another MX record with a host name of `Domino3` and a preference number of 30.
10. Click on **OK** a second time to exit the Properties window.

Note

Steps 8 and 9 are optional. By adding three MX records, you provide backup mail servers in the domain. If `DOM400` is not available, the firewall will send the mail to the next preferred mail server, `DOMINO2`. To provide complete support, you should configure the other systems as secondary DNS servers for the domain.

You have now successfully created the MX record for `domain.com`.

6.2.5 Configuring the internal DNS to forward the queries to the firewall

The internal DNS cannot answer the queries that are intended for the Internet. It needs to be linked with the DNS in the firewall.

If e-mail is sent to `somebody@us.ibm.com`, it first goes to the internal SMTP server. Then, it is forwarded to the firewall. From the firewall, it is sent to the Internet.

To set up DNS forwarding, you must change the DNS properties. You should start at the DNS Server Configuration window shown in Figure 263. Use the following procedure to change the properties of the DNS:

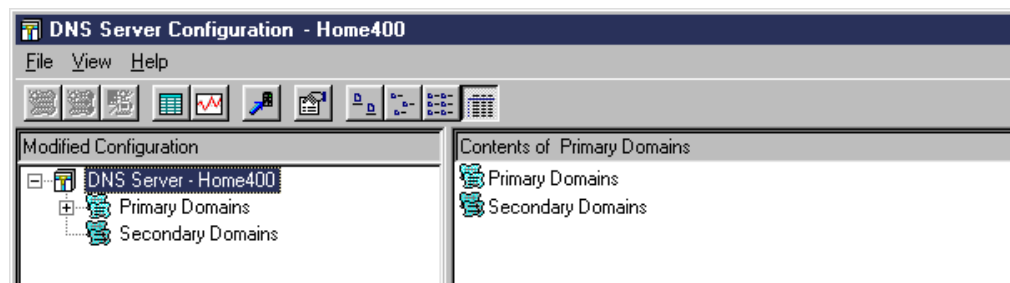


Figure 263. Configuring the internal DNS to forward queries to the firewall

1. Right-click **DNS Server - Home400**.
2. Select **Properties**.
3. Click the **Forwarders** tab. The window shown in Figure 264 on page 202 is displayed.

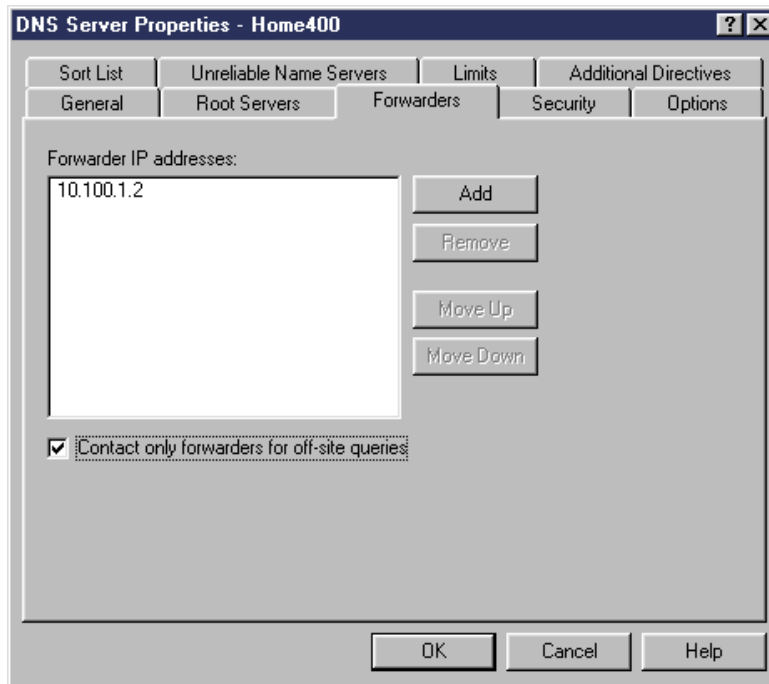


Figure 264. Adding the IP address of the firewall to the forwarders list

4. Click the **Add** button.
5. Enter the secure IP address of the firewall.
6. Check **Contact only forwarders for off-site queries**.
7. Click **OK**.

The DNS configuration is now ready to handle your SMTP mail. Stop and start the DNS server, or click **File->Update Server** to update the DNS server configuration and make your configuration available.

6.3 Configuring IBM Firewall for AS/400 (FW4MAIL)

This section describes the tasks that you must perform to configure IBM Firewall for AS/400 to handle multiple domains on multiple mail servers.

6.3.1 Scenario network configuration

Figure 265 on page 203 shows the network configuration used in this scenario. In this portion of the scenario, we use an Integrated Netfinity Server to run the IBM Firewall for AS/400. The network diagram would be the same if we used IBM eNetwork Firewall for Windows NT. The *Internal LAN and one LAN adapter make up the secure side of the Network. The other LAN adapter is used to connect to the ISP router.

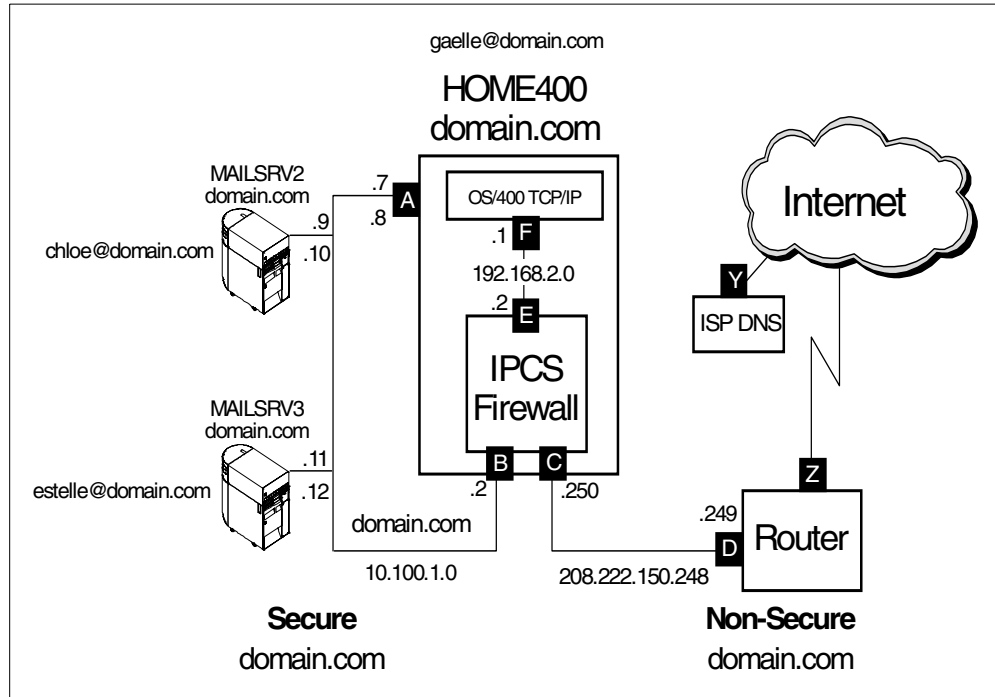


Figure 265. Single domain with fanout - IBM Firewall for AS/400

6.3.2 Task summary

The following list summarizes the tasks used to configure IBM Firewall for AS/400:

1. Install IBM Firewall for AS/400.
2. Perform the basic configuration.

6.3.3 Installing IBM Firewall for AS/400 (FW4MAIL)

Install the firewall at the local site using the instructions in the manual *Getting Started with IBM Firewall for AS/400*, SC41-5424. A summary of the installation parameters is shown on the Complete the Firewall Installation summary page in Figure 266 on page 204.



Complete the Firewall Installation

Review the information that you have entered. Make any changes on this page. When you are sure that the information is correct, click the **Install** button to complete the firewall installation. This step takes several minutes to run. Please be patient.

Firewall Name	FW4MAIL							
Firewall Resource Name	CC02							
Router IP Address	208	222	150	249				
Route Destination	Subnet Mask		Next Hop					
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>					
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>					
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>					
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>					
	Port 1	Port 2						
LAN Type	Token Ring (16Mb)	Token Ring (16Mb)						
Adapter Address	400000000037	400000000250						
IP Address	10	100	1	2	208	222	150	250
Subnet Mask	255	255	255	0	255	255	255	248

Figure 266. Firewall Installation summary page (FW4MAIL)

Start the firewall by clicking the **Start** button (Figure 267).



Start the Firewall

The firewall takes several minutes to start. Please be patient. Click **Start** to start the firewall.



Figure 267. Starting the firewall (FW4MAIL)

6.3.4 Performing basic configuration (FW4MAIL)

Perform the basic configuration of the local firewall. For further information, refer to *Getting Started with IBM Firewall for AS/400, SC41-5424*, and redbook *AS/400 Internet Security: IBM Firewall for AS/400, SG24-2162*.

In the Review Configuration, be aware that the *Secure Mail Server* and the *Secure Domain* refer to the internal mail domain name. The SMTP domain name in the inbound e-mail (the value to the right of the @ symbol) is changed to the value in the Secure Mail Server column. This value must match the SMTP mail

address setup for the user on the secure mail server. In our scenario, these values have to be exactly the same because of the domain names we select for our internal users. The value in the Secure Mail Server parameter is used in an MX record DNS query to find the SMTP server that processes the mail. If the query fails, an A record DNS query is done for the value. If an IP address is returned, the mail is routed to the mail server. In most cases, it is easiest to use the same value for the Secure Mail Server and the Secure Domain parameters and let the internal DNS MX records point to the secure mail server system. Refer to Table 26 on page 196 for information about the domain name and secure mail server name.

If you do not have a DNS server in the secure network, this technique will not work. You must specify the fully qualified name of the secure mail server (for example, `hostname.domain.com`) in the Secure Mail Server column. This means that the e-mail address of the users will be in the form `userid@hostname.domain.com`.

We recommend that you link the firewall DNS with multiple DNS in the outside world. If one fails, you can still continue to send e-mail and surf the Web. In our scenario, the three DNS belong to the ISP.

For more information about IBM Firewall for AS/400, refer to Appendix D, “Firewall concepts” on page 349.

Figure 268 and Figure 269 on the following pages show the Review Configuration for FW4MAIL. Refer to Figure 265 on page 203 for the scenario network configuration.



Review Configuration

Review the information that you have entered. Make any changes on this page. When you are sure that the information is correct, print the page for future reference. This creates all the firewall configuration settings. This may take a few minutes to run, so please be patient.

Your AS/400 is: HOME400.DOMAIN.COM

Your firewall is: FW4MAIL

Secure domain name servers:

10.100.1.7

Secure Port	IP Address	Subnet Mask
<input checked="" type="radio"/> Port 1	10.100.1.2	255.255.255.0
<input type="radio"/> Port 2	208.222.150.250	255.255.255.248

Secure Mail Server	Secure Domain	Public Domain
domain.com	domain.com	domain.com

Name Server	IP Address
dns1.isp.com	194.41.0.4
dns2.isp.com	128.9.0.107
dns3.isp.com	192.33.4.12

Figure 268. Basic firewall configuration summary page for FW4MAIL (Part 1 of 2)

Public Server	Public IP Address	Private IP Address

Services	Proxy	SOCKS	NAT
HTTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HTTPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FTP (passive)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FTP (active)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Telnet	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Secure Telnet		<input type="checkbox"/>	<input type="checkbox"/>
Gopher	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WAIS			<input type="checkbox"/>
IRC		<input type="checkbox"/>	<input type="checkbox"/>
RealAudio			<input type="checkbox"/>
Lotus Notes		<input type="checkbox"/>	<input type="checkbox"/>
LDAP		<input type="checkbox"/>	<input type="checkbox"/>
Secure LDAP		<input type="checkbox"/>	<input type="checkbox"/>
Server Mapper		<input type="checkbox"/>	<input type="checkbox"/>
DRDA		<input type="checkbox"/>	<input type="checkbox"/>
POP3 Mail		<input type="checkbox"/>	<input type="checkbox"/>
NNTP		<input type="checkbox"/>	<input type="checkbox"/>
Secure NNTP		<input type="checkbox"/>	<input type="checkbox"/>

If you selected any NAT services, then specify the translation of private to public IP addresses.

NAT	IP Address	Mask
Private	10.100.1.2	255.255.255.0
Public		

OK Cancel

Figure 269. Basic firewall configuration summary page for FW4MAIL (Part 2 of 2)

The firewall is now ready for you to perform the basic configuration. Complete these steps:

1. Click **OK**. A confirmation page is shown, indicating that the firewall is configured (Figure 270).



You have successfully configured the firewall. The next step is to restart the firewall servers so that your configuration changes take effect. This will only take a short time. Do you want to restart the firewall?

Figure 270. Confirmation that the firewall is configured

2. Click **Yes**.

IBM Firewall for AS/400 configuration is now ready.

For more information about IBM Firewall for AS/400, refer to Appendix D, “Firewall concepts” on page 349.

6.4 Configuring IBM eNetwork Firewall for Windows NT (FW4NT)

This section describes the tasks that you must perform to configure IBM eNetwork Firewall for Windows NT to handle multiple domains on multiple mail servers.

6.4.1 Scenario network configuration

Figure 271 on page 209 shows the network configuration for this scenario.

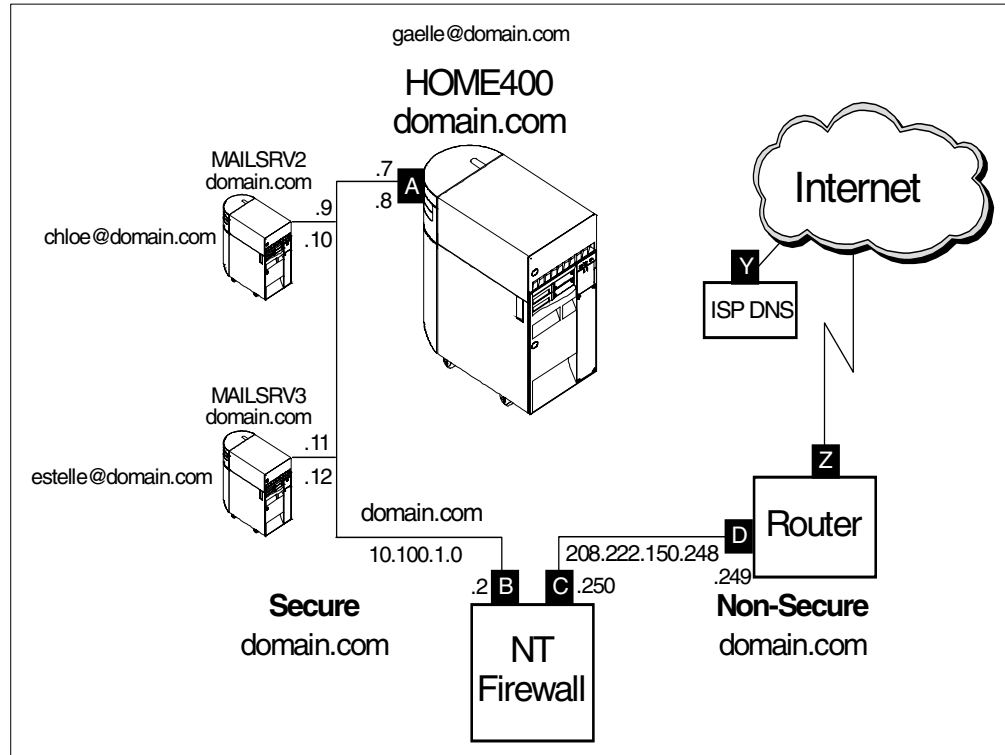


Figure 271. Single domain with fanout - IBM eNetwork Firewall for Windows NT

6.4.2 Task summary

The following list summarizes the tasks used to configure IBM eNetwork Firewall for Windows NT:

1. Install IBM eNetwork Firewall for Windows NT.
2. Setup IBM eNetwork Firewall for Windows NT.

6.4.3 Installing IBM eNetwork Firewall for Windows NT (FW4NT)

Install the firewall on the Windows NT PC using the instructions in *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT*, SG24-5209.

If you do not have this redbook and do not have Internet access to download it, complete the following steps:

1. Install the Windows NT server operating system.
2. Install the DNS server for the Windows NT server.
3. Install Service Pack 4 for the Windows NT server. Use Service Pack 5 if it is available. Service Pack 4 is required. Do not install IBM eNetwork Firewall for Windows NT on the system without the above service pack.
4. Create a local user with administrator authority.
5. Install the IBM NDIS intermediate driver.
6. Activate IP forwarding in the TCP/IP parameters.
7. Install the firewall product.

6.4.4 Setting up IBM eNetwork Firewall for Windows NT

Complete the following steps to set up IBM eNetwork Firewall for Windows NT:

1. Run the **Configuration Client** in the IBM Firewall folder.
2. Log in with a user that has administrator authority.
3. To start basic configuration, click **Setup Wizard** in the **Help** menu (Figure 272).

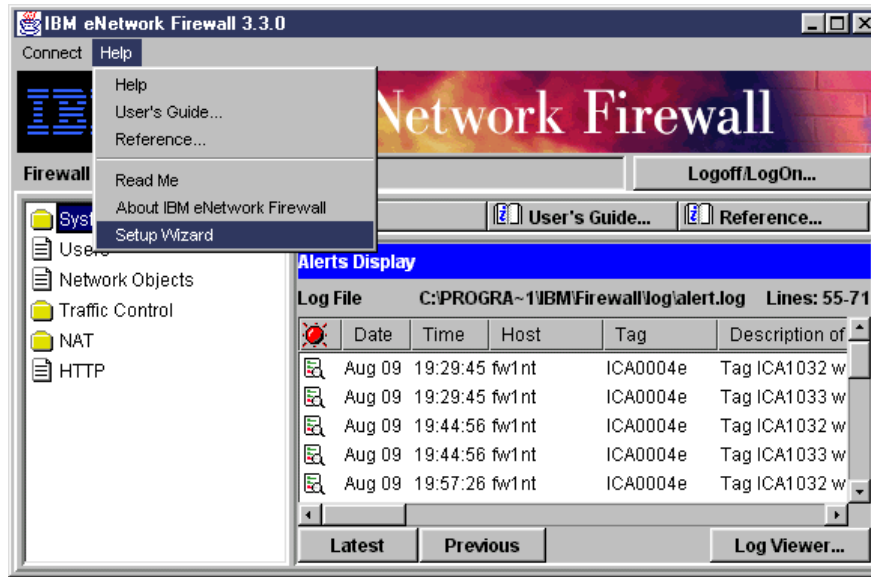


Figure 272. Starting firewall wizard

4. The Welcome window appears (Figure 273). Read the window carefully.

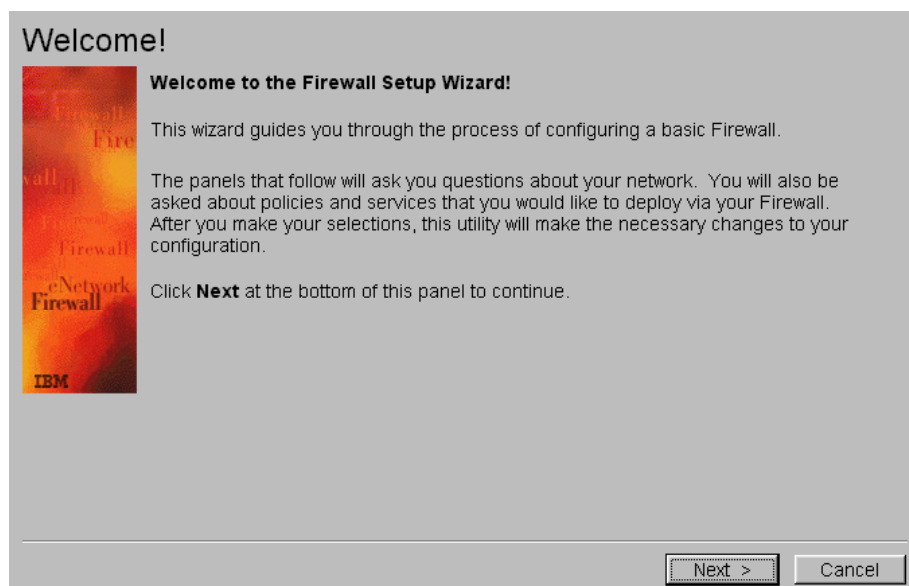


Figure 273. Welcome screen firewall wizard

5. Click **Next**. The window shown in Figure 274 on page 211 appears. Read the window carefully.

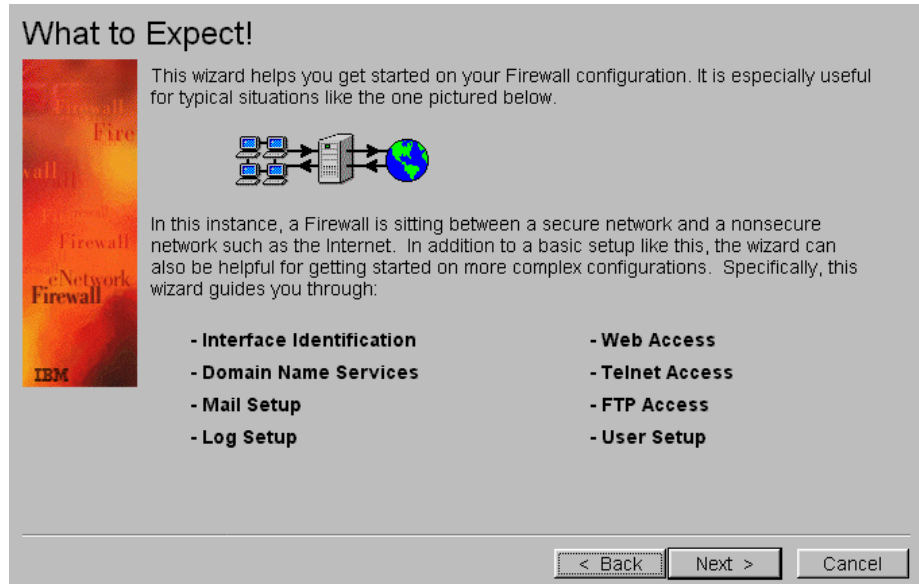


Figure 274. What to Expect firewall wizard

6. Click **Next**. The window shown in Figure 275 appears. Read the window carefully.

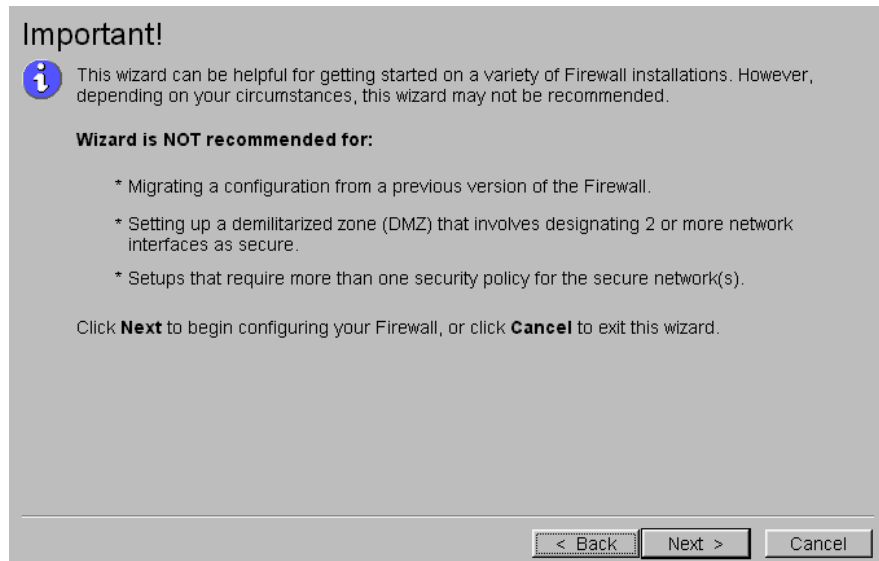


Figure 275. Important notice firewall wizard

7. Click **Next**. The window shown in Figure 276 on page 212 appears. Choose the secure interface.

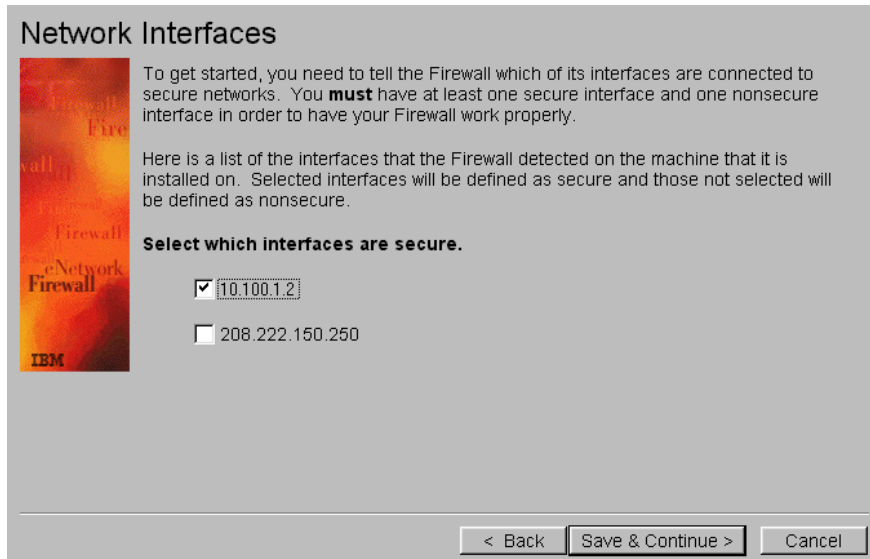


Figure 276. Network interface selection

8. Click **Save & Continue**. The window shown in Figure 277 appears.

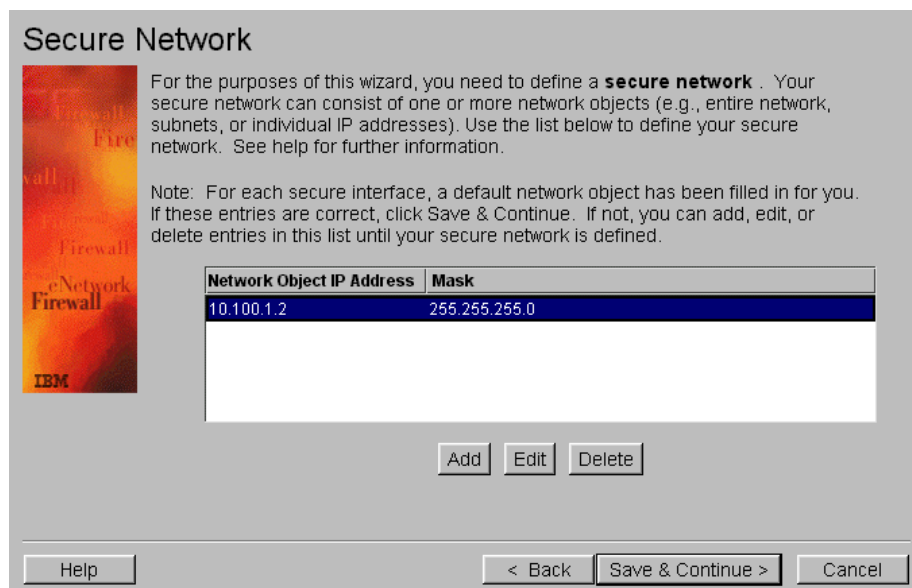


Figure 277. Secure network configuration

9. Define your secure network. In the window shown in Figure 277, the wizard guesses that your secure network is any IP address that starts with 10.100.1. Click **Save & Continue**. The window shown in Figure 278 on page 213 appears.

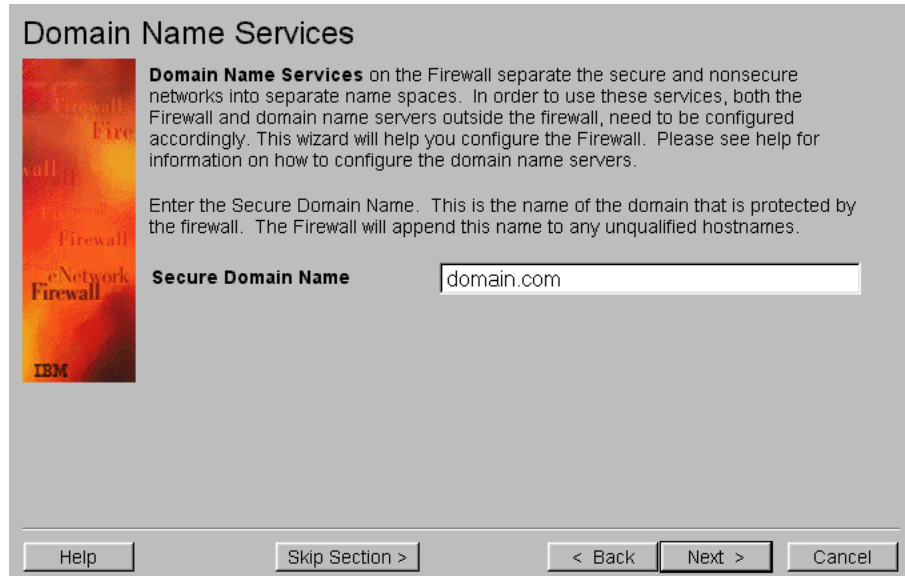


Figure 278. Domain Name Services

10. Enter the name of your internal domain name. This domain is protected by your firewall. Click **Next**. The window shown in Figure 279 appears.

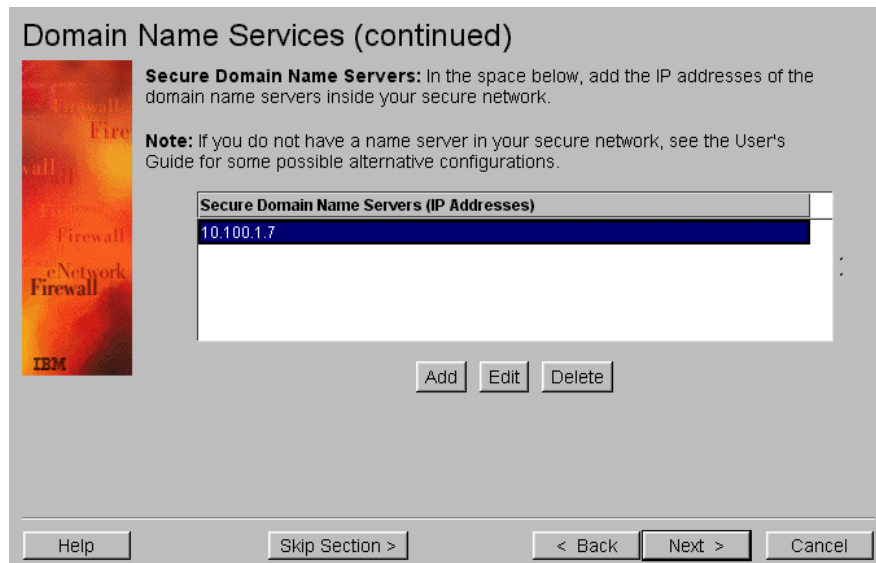


Figure 279. Secure DNS IP address

11. Enter the IP Address of the secure internal DNS. Click **Next**. The window shown in Figure 280 on page 214 appears.

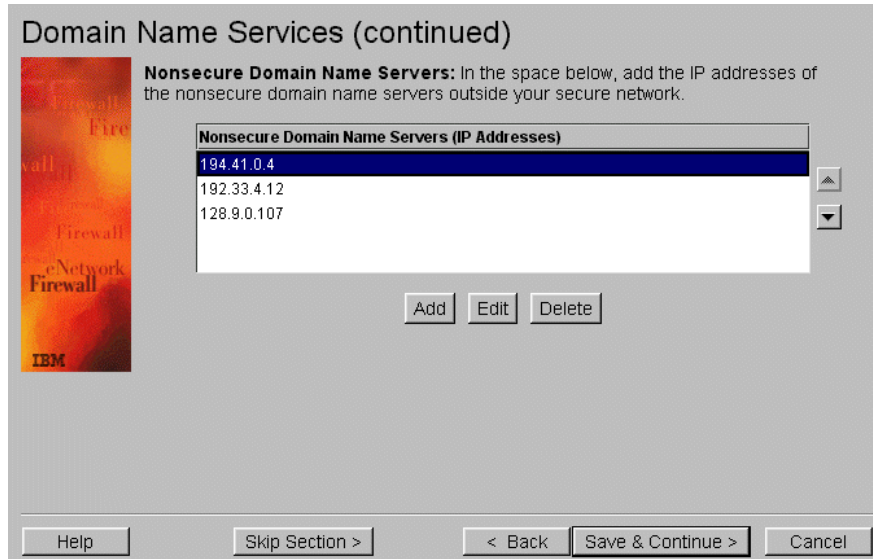


Figure 280. Non-Secure DNS IP addresses

12. Click **Add**.
13. Enter the IP address of the non-secure DNS (ISP DNS). Click **Next**.
14. Repeat steps 12 and 13 if the firewall DNS is linked with more DNS (recommended).
15. Click **Save & Continue**. The window shown in Figure 281 appears.

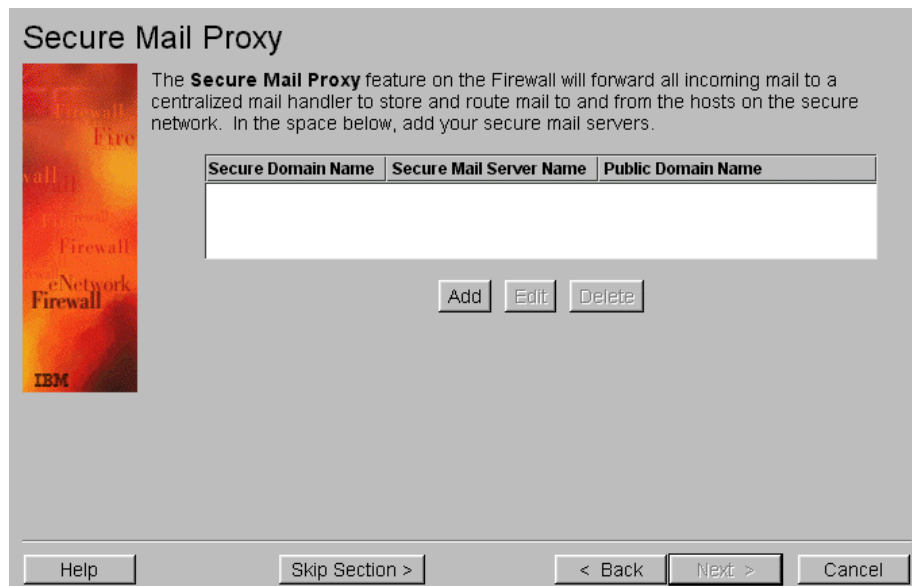


Figure 281. Secure Mail Proxy

16. Click **Add**. The window shown in Figure 282 on page 215 appears.



Figure 282. Adding a secure mail server

17. Enter your Secure Domain Name, Secure Mail Server Name, and Public Domain Name. Refer to Table 26 on page 196 for information about the domain name and secure mail server name. Click **Save & Continue**. The window shown in Figure 283 appears.



Figure 283. Secure Mail Proxy

18. Click **Next**. The window shown in Figure 284 on page 216 appears.



Figure 284. Security policies configuration

19. The marked options that you see under Policy Options are recommended for most firewall installations. Click **Save & Continue**. The window shown in Figure 285 appears.



Figure 285. Web Access

20. Specify whether to allow Internet access to users. Click **Next**. The window shown in Figure 286 on page 217 appears.



Figure 286. Web Access via Proxy, Socks, or Filtered Only

21. Specify which Web access matches best with your company. Click **Next**. The window shown in Figure 287 appears.



Figure 287. Web Access services

22. Select which services are allowed. Click **Save & Continue**. The window shown in Figure 288 on page 218 appears.

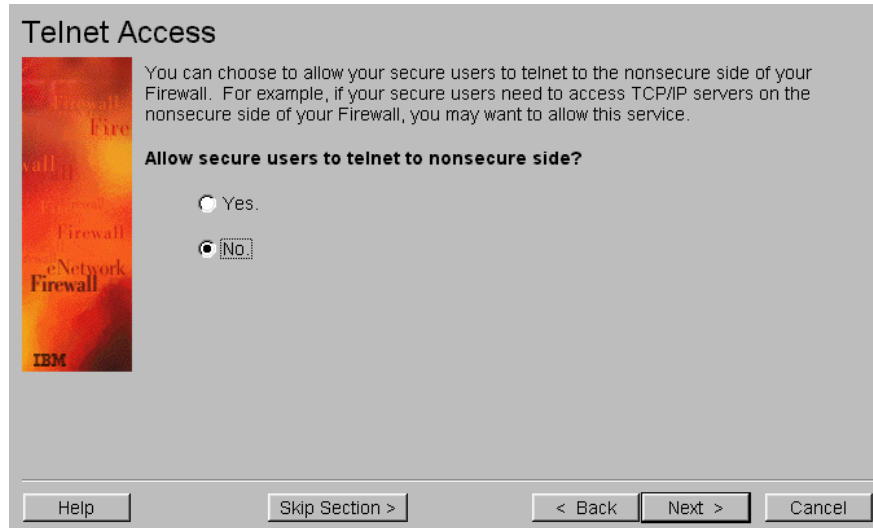


Figure 288. Telnet Access

23. Specify whether to allow Telnet access on the non-secure port of the firewall. Click **Next**. The window shown in Figure 289 appears.

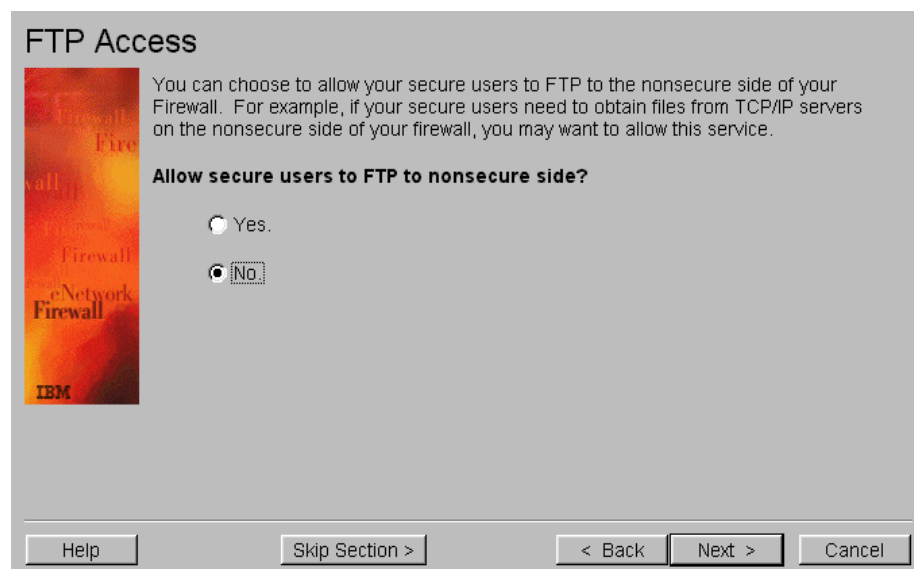


Figure 289. FTP Access

24. Specify whether to allow FTP access on the non-secure port of the firewall. Click **Next**. The window shown in Figure 290 on page 219 appears.

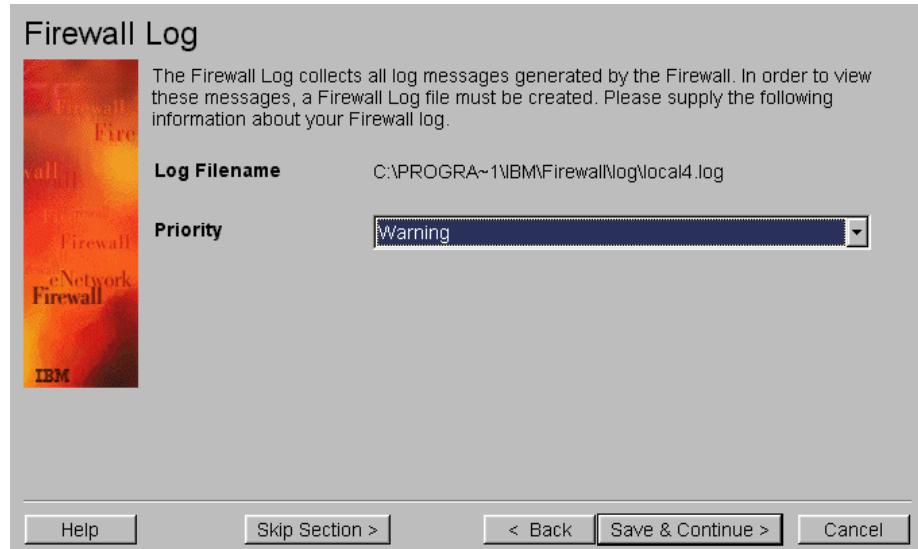


Figure 290. Firewall Log

25. Choose which level of logs are stored on the firewall database. Click **Save & Continue**. The window shown in Figure 291 appears.

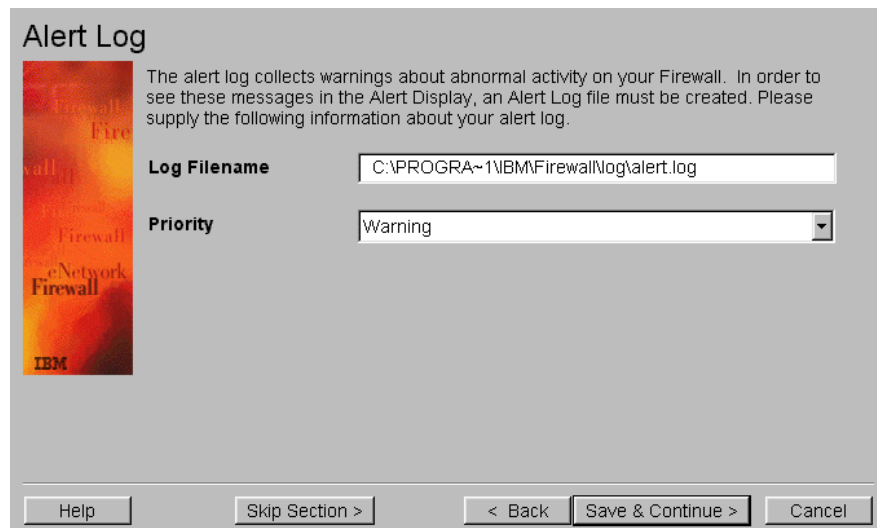


Figure 291. Alert Log

26. Choose which level of logs are stored on the alert database. Click **Save & Continue**. The window shown in Figure 292 on page 220 appears.

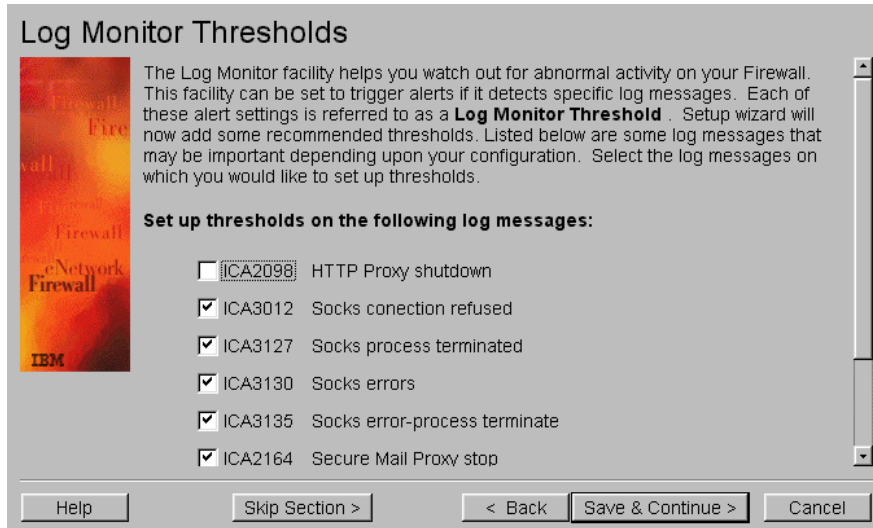


Figure 292. Log Monitor Thresholds

27. Select the thresholds. Click **Save & Continue**. The window shown in Figure 293 appears.

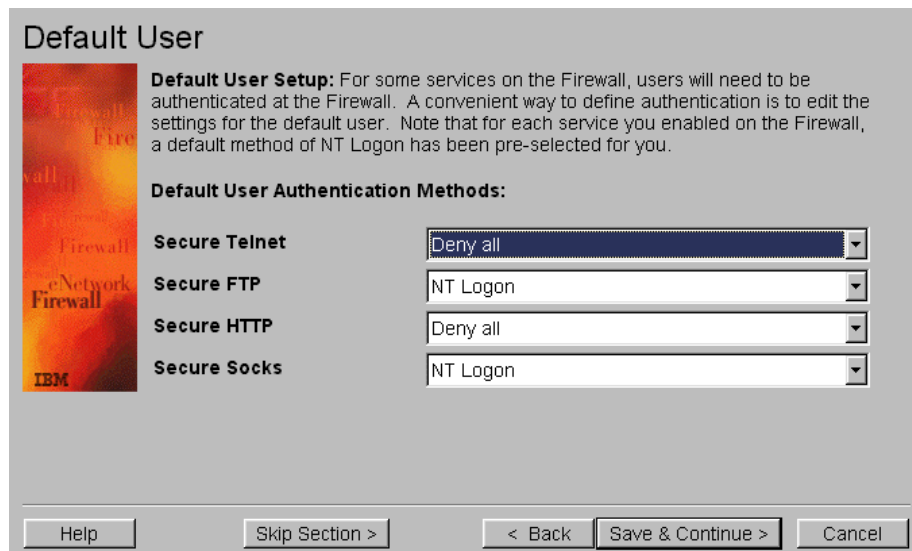


Figure 293. Default User setup

28. For some services, a firewall user needs to be authenticated. Click **Save & Continue**. The window shown in Figure 294 on page 221 appears.

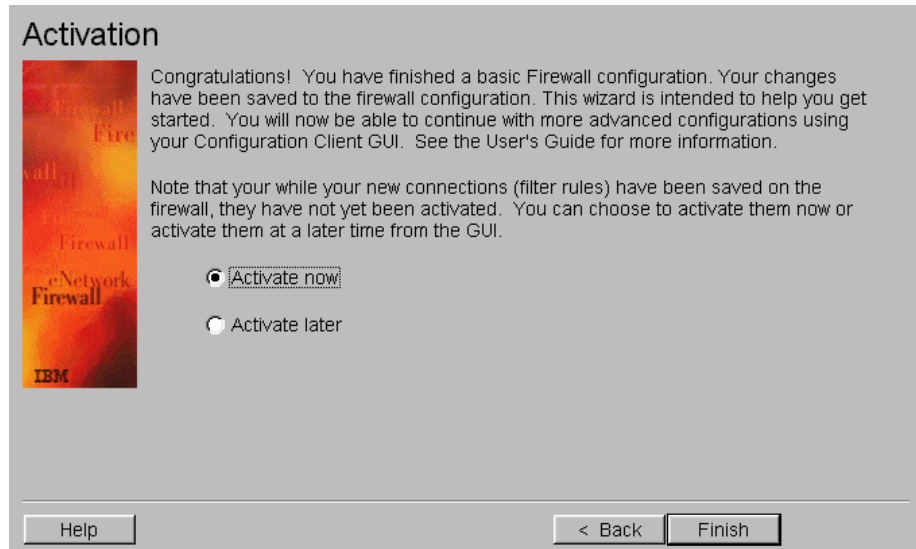


Figure 294. Setup Activation

29. Specify whether to activate your configuration now or at a later time. Click **Finish**.

IBM eNetwork Firewall for Windows NT configuration is now ready.

For more information about IBM eNetwork Firewall for Windows NT, refer to Appendix D, “Firewall concepts” on page 349.

6.5 Planning the Domino server on AS/400 systems

This section describes the tasks that you must perform to plan Domino servers on AS/400 systems.

6.5.1 Planning considerations

There are several ways to implement a Domino server on an AS/400 system to handle SMTP mail:

- SMTP server on the Domino server
- SMTP server with MSF on the AS/400 system
- SMTP server with MSF on the AS/400 system and on the Domino server

The first configuration, SMTP server on the Domino server, is the one we are implement in this scenario.

The second configuration, SMTP server with MSF on the AS/400 system, is documented in 5.9, “Configuring Domino with MSF on the AS/400 system” on page 183.

The third possibility needs specific configurations. If you need to use both the SMTP server on the AS/400 system and the SMTP server on the Domino server, you have to bind each application to a specific IP address. Refer to the Dual Stack PTF cover letter. In V4R2, this is supported by PTF SF55697. In V4R3, this is supported by PTF SF58661. A PTF is under development for V4R4. These PTFs are

OS/400 PTFs that are used to add the feature. The cover letter for the PTF also lists a corresponding co-requisite PTF from the POP snap-ins.

Figure 295 on page 222 shows the mail flow between the Internet, the firewall, and the Domino servers located inside the secure network. The process is explained here:

1. The SMTP messages coming from the Internet cross the firewall and are delivered to DOM400.
2. DOM400 keeps the messages addressed to itself and routes the other messages to DOMINO2 and DOMINO3.

If the optional MX records were configured as shown in 6.2.4, “Configuring the MX record for your domain” on page 200, DOMINO2 and DOMINO3 may receive mail from the firewall if DOM400 is not available.

3. For internal mail, the three Domino servers communicate in Notes Remote Procedure Call (NRPC). The link between the Domino servers is configured in the address book through Connection Documents.
4. For outbound mail destined for the Internet, each Domino server sends its own SMTP mail through the firewall. Processing this way minimizes the chance of having a bottleneck in your Domino gateway.

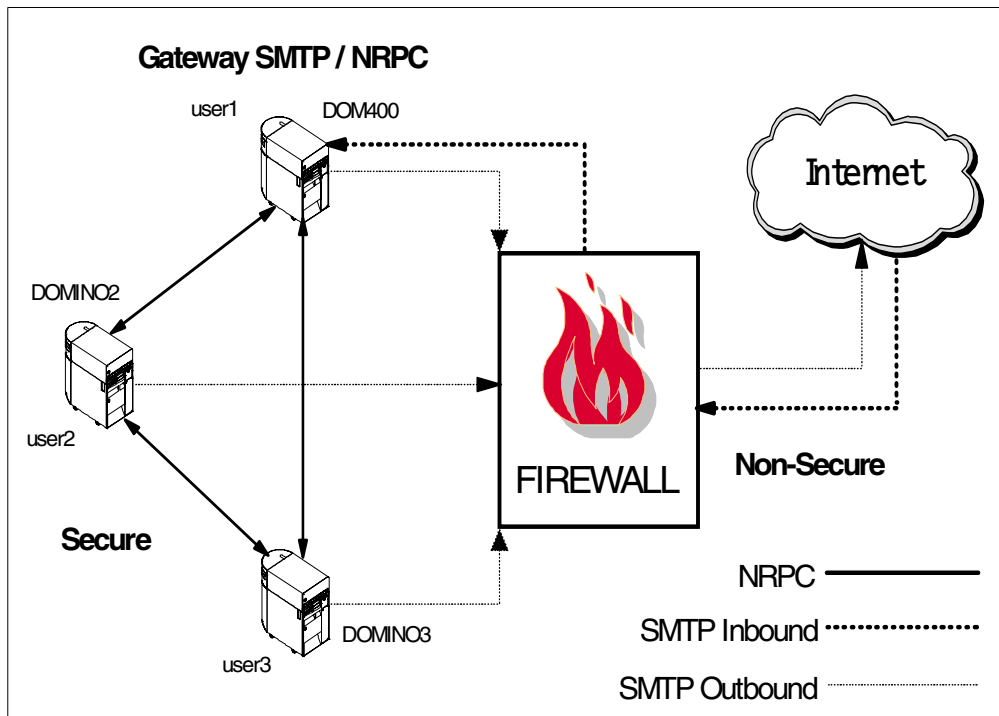


Figure 295. Mail flow between the Domino servers and the firewall

In Table 30 on page 223, the Domino domains are referred to as the AS/400 name, but it can be any other name. We do not use *ORG (DOMAIN) because this means that we have one Domino domain and one address book. Configuring with different Domino domains allows each Domino server to have its own address book and to be independent of the other servers in the network.

Table 30 shows the configuration values we used for the three Domino servers.

Table 30. Configuration values for DOM400, DOMINO2, and DOMINO3

Values	DOM400	DOMINO2	DOMINO3
AS/400	HOME400	MAILSRV2	MAILSRV3
IP Domino address	10.100.1.8	10.100.1.10	10.100.1.12
IP Host name	dom400	domino2	domino3
IP Domain name	domain.com	domain.com	domain.com
Server name	DOM400/DOMAIN	DOMINO2/ORG2	DOMINO3/ORG3
Organization name	DOMAIN	ORG2	ORG3
Domino domain	HOME400	MAILSRV2	MAILSRV3
as/400 data directory	/domino/dom400/data	/domino/domino2/data	/domino/domino2/data
Internet packages	*SMTP	*SMTP	*SMTP
SMTP services	*DOMINO	*DOMINO	*DOMINO
User.id	admin_dom400	admin_domino2	admin_domino3
Cert.id	domain.id	org2.id	org3.id
Server.id	dom400.id	domino2.id	domino3.id
PAB Replica name	dom400_names	domino2_names	domino3_names

Use Table 31 to record the values you need for your configuration.

Table 31. Configuration values for user systems

Values			
AS/400			
IP Domino address			
IP Host name			
IP Domain name			
Server name			
Organization name			
Domino domain			
as/400 data directory			
Internet packages			
SMTP services			

Values			
User.id			
Cert.id			
Server.id			
PAB Replica name			

6.6 Configuring the three Domino servers

The task you must perform to set up the three Domino servers is similar to the task documented in 3.7, “Configuring the Domino server for mail” on page 71. In this section, we refer you to that procedure and only document the steps that are different for this scenario.

6.6.1 Task summary

The following list summarizes the tasks used to implement the Domino server on the AS/400 HOME400:

1. Set up HOME400 to handle Domino.
2. Install the Domino server on HOME400.
3. Install Domino Administrator on your workstation.
4. Set up your workstation to administer Domino.
5. Configure the Domino server for SMTP mail.
6. Link the Domino server with the firewall.
7. Create Lotus Notes mail users.

The Domino servers on HOME400, MAILSRV2, and MAILSRV3 have the same configuration. We use Domino server on HOME400 as a reference. Perform the procedures from 3.7.3, “Setting up HOME400 to handle Domino” on page 72, through 3.7.6, “Setting up your workstation to administer Domino” on page 78. This guides you through tasks 1 through 4 from the task list. Return here when you reach “Stop here” on page 82. Refer to Table 30 on page 223 for the configuration values. Repeat the procedures three times, once for each set of values in the table.

The configuration for inbound Internet mail is already made in the firewall and DNS server as follows:

- In the firewall, the secure SMTP server (DOM400) is already known by the SMTP relay function.
- In the secure DNS, the MX record (mail exchanger) for *domain.com* is configured to point to DOM400.

No additional configuration is needed. All mail addressed to *domain.com* is routed to the Domino server DOM400.

6.6.2 Configuring the Domino server for SMTP mail

This section describes how to set up the Domino server to handle SMTP mail. Refer to Table 30 on page 223 for the configuration values. Use the values in the column labeled DOM400.

On the Domino Administrator desktop, perform the following steps. Use the example shown in Figure 296 as a guide for the first five steps.

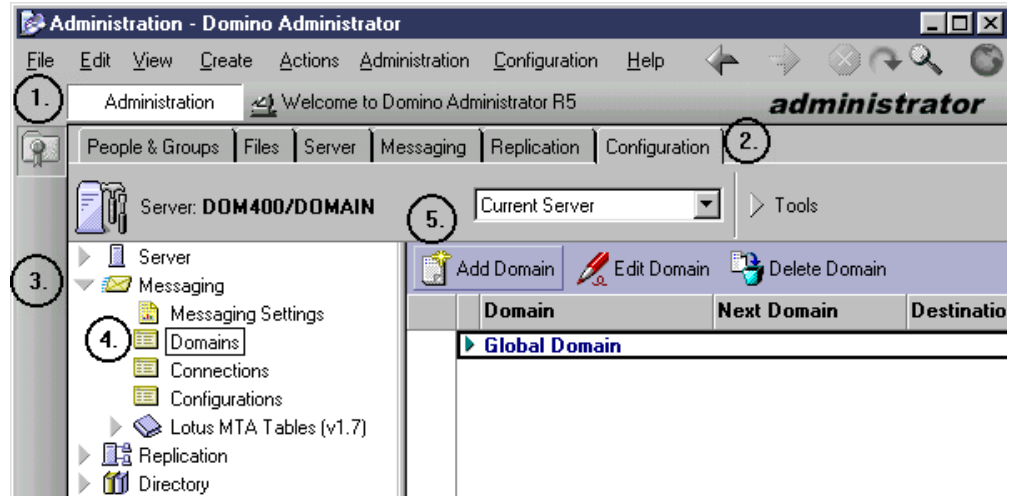


Figure 296. Domain document

1. Click the **Administration** button (1).
2. Click the **Configuration** Tab (2).
3. Open **Messaging** in the navigation tree (3).
4. Click **Domains** (4).
5. Click the **Add Domain** button (5). The display shown in Figure 297 appears.

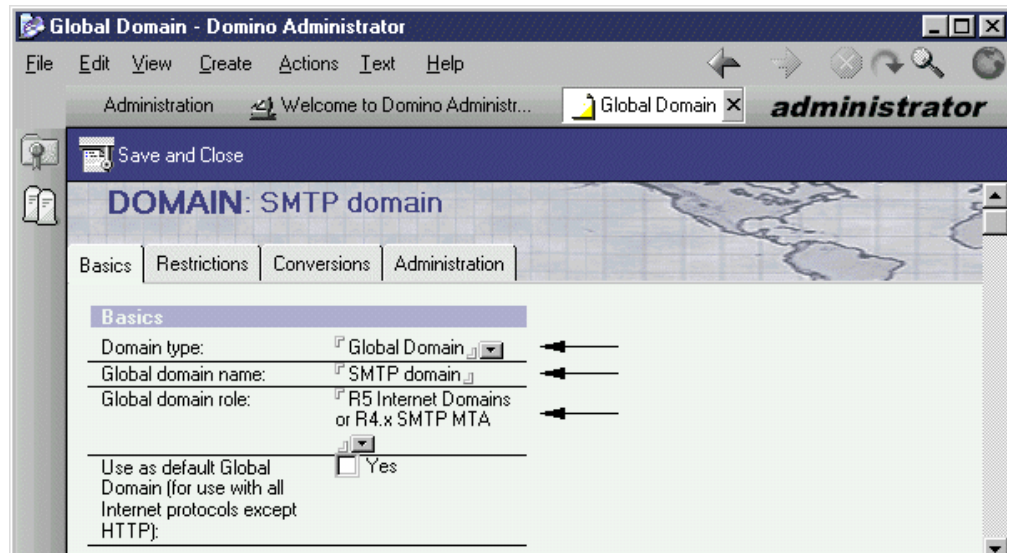


Figure 297. Domain document - Basics

6. Select **Global Domain** for Domain type.
7. Enter `SMTP Domain` for Global domain name.
8. Select **R5 Internet Domains** for Global domain role.
9. Click on the **Conversions** tab. The display shown in Figure 298 on page 226 appears.

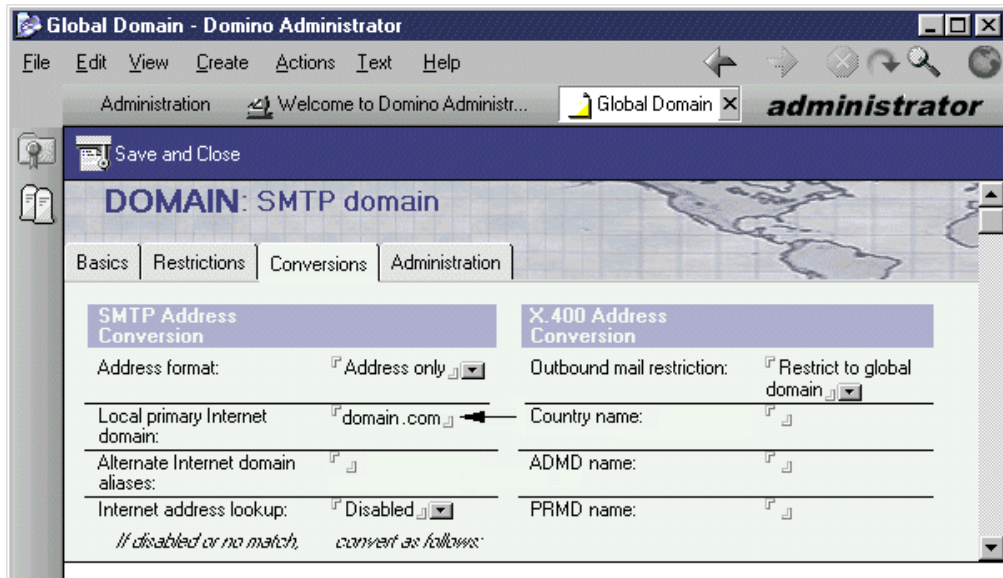


Figure 298. Domain document - Conversion

10. Enter `domain.com` for Local primary Internet domain.
11. Leave the Alternate Internet domain aliases field blank.
12. Click **Save and Close**. You return to a window similar to the example shown in Figure 296 on page 225.

Use Figure 299 as a guide for the next three steps.

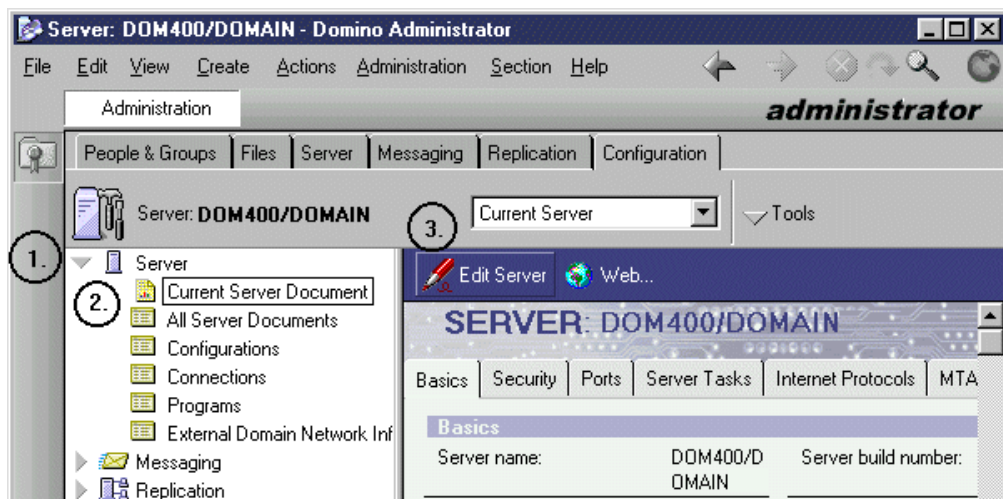


Figure 299. Server document

13. Open **Server** in the navigation tree (1).
14. Select **Current Server Document** (2).
15. Click the **Edit Server** button (3). The display shown in Figure 300 on page 227 appears.

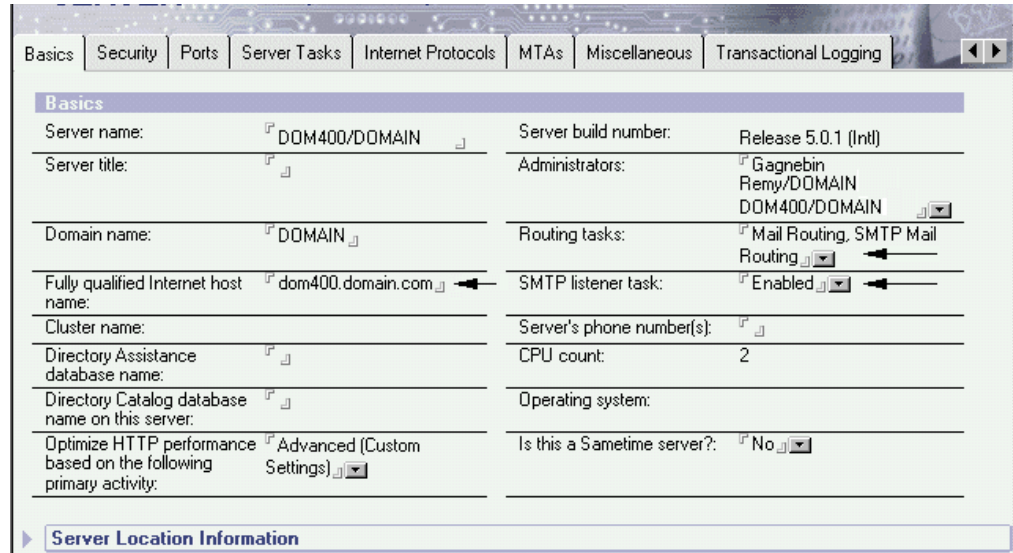


Figure 300. Server document - Basics

16. The Fully qualified Internet host name *must* match the Domino server name.

17. Verify that the SMTP listener task is *Enabled*.

18. Verify that the Routing tasks are *Mail Routing* and *SMTP Mail Routing*.

19. Click **Save and Close**.

You have now configured DOM400 to handle Internet mail using SMTP. Repeat these steps for DOMINO2 and DOMINO3.

6.6.3 Linking the Domino server with the firewall

To link the Domino SMTP server with the firewall, perform the following steps. Use the example shown in Figure 301 as a guide for the first three steps.

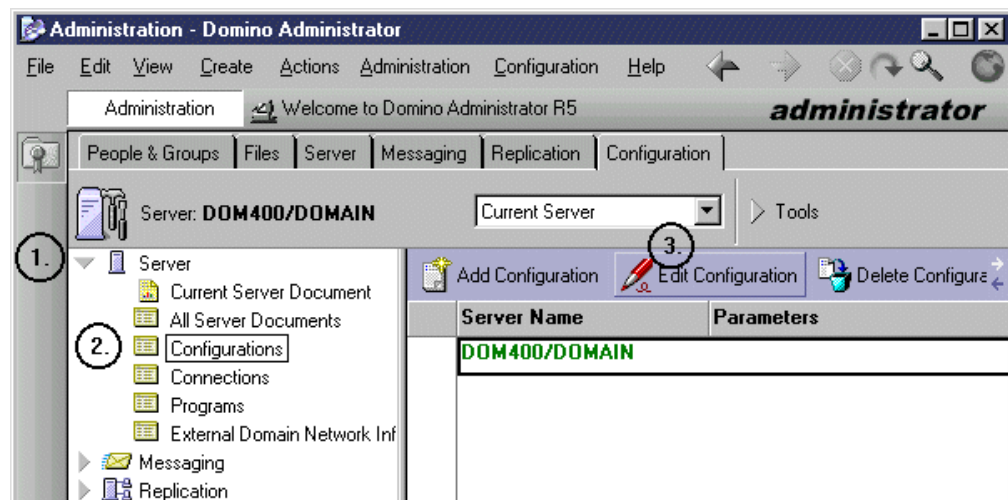


Figure 301. Configuration document

1. Open **Server** in the navigation tree (1).

2. Click the **Configurations** tab (2).

- Click the **Edit Configurations** button (3). The display shown in Figure 302 appears.

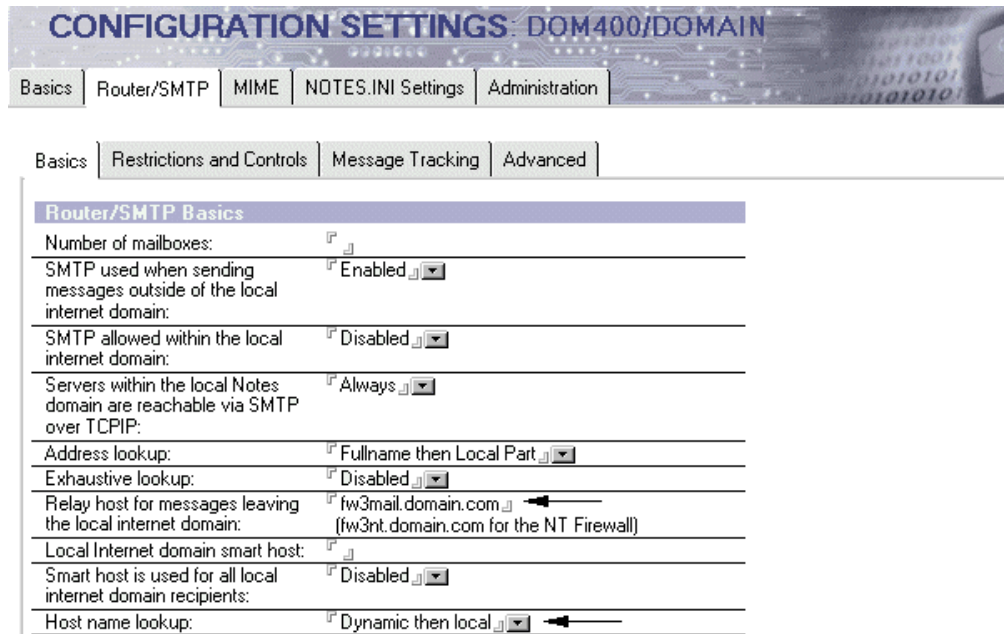


Figure 302. Configuration document - Router / SMTP

- Click the **Router/SMTP** tab.
- Enter the firewall name for Relay host for messages leaving the local Internet domain.
- Verify that the Host name lookup is set to `Dynamic then local`.
- Click **Save and Close**.

You have now linked the Domino SMTP server with the SMTP relay function of your firewall.

Repeat these steps for DOMINO2 and DOMINO3.

6.7 Linking and trusting the Domino servers together

This section describes the tasks that you must perform to link and trust the three Domino servers. The Domino servers (DOM400, DOMINO2, and DOMINO3) have the same configuration. We use Domino server DOM400 as a reference. Follow the instructions in this section, and refer to Table 30 on page 223 for the configuration values.

6.7.1 Task summary

The following list summarizes the tasks used to link and trust the three Domino servers together:

- Create domain documents.
- Create connection documents.
- Cross certify the Domino servers.

6.7.2 Creating domain documents

This section describes how to create domain documents. The domain document describes the type and the relationship you have with this domain. Refer to Table 30 on page 223 for the configuration values.

Complete the following steps to create domain documents. On the Domino Administrator desktop, refer to Figure 303 for the first five steps.

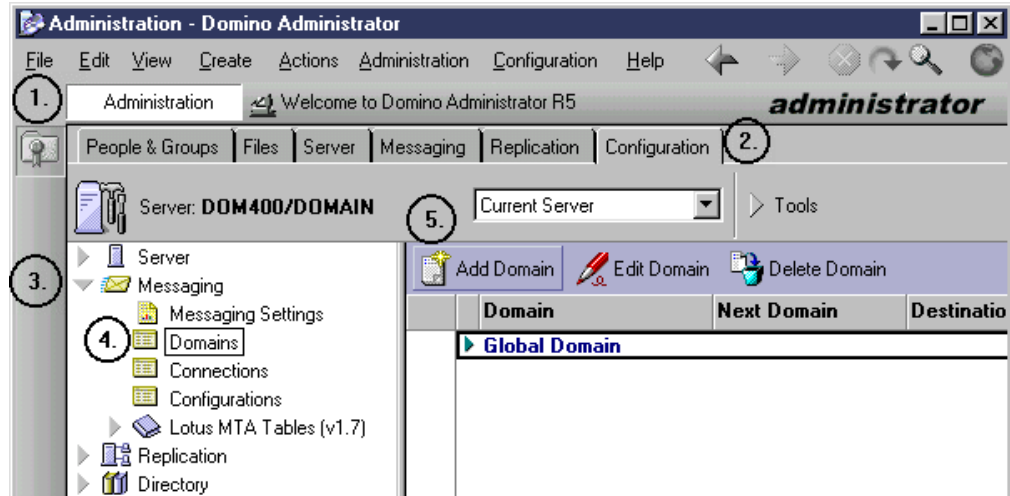


Figure 303. Domain document

1. Click the **Administration** button (1).
2. Click the **Configuration** tab (2).
3. Open **Messaging** in the navigation tree (3).
4. Click **Domains** (4).
5. Click the **Add Domain** button (5). The display shown in Figure 304 appears.

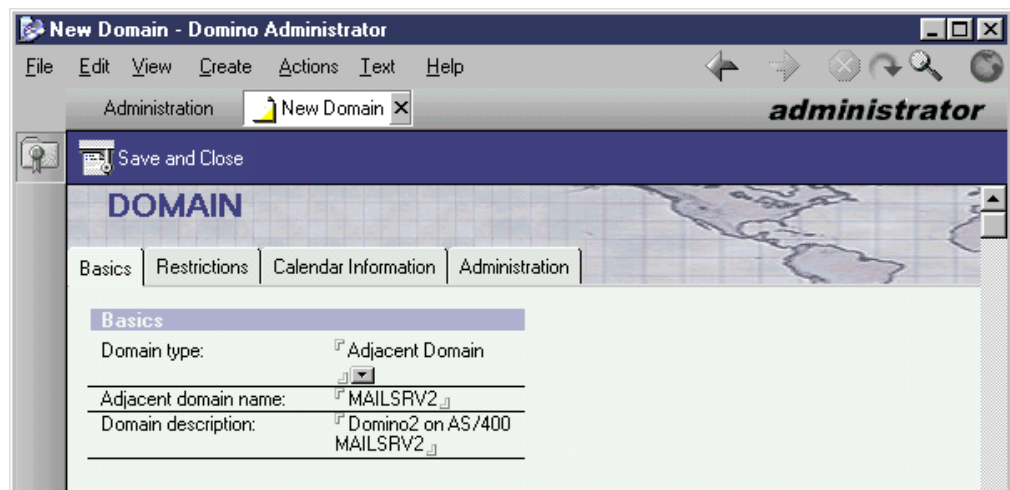


Figure 304. Domain document - Basics

6. Select **Adjacent Domain** for Domain type.
7. Enter MAILSRV2 for Adjacent domain name.

8. Enter your Domain description.

9. Click **Save and Close**.

You have now created the Domain document. This tells DOM400 the type and the relationship you have with the MAILSRV2 domain. Now we create a new domain document for MAILSRV3.

10. Click the **Add Domain** button. The display shown in Figure 305 appears.

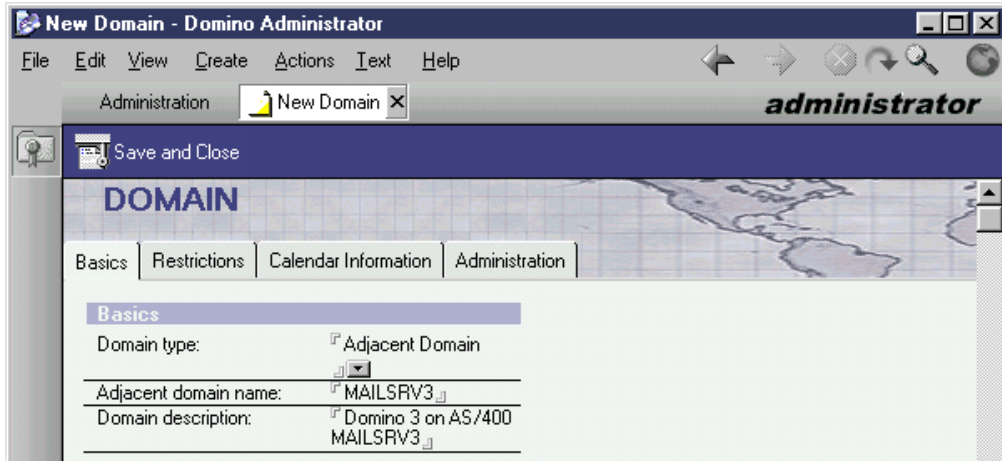


Figure 305. Domain document - Basics

11. Select **Adjacent Domain** for Domain type.

12. Enter MAILSRV3 for Adjacent domain name.

13. Enter your domain description.

14. Click **Save and Close**. The display shown in Figure 306 appears.

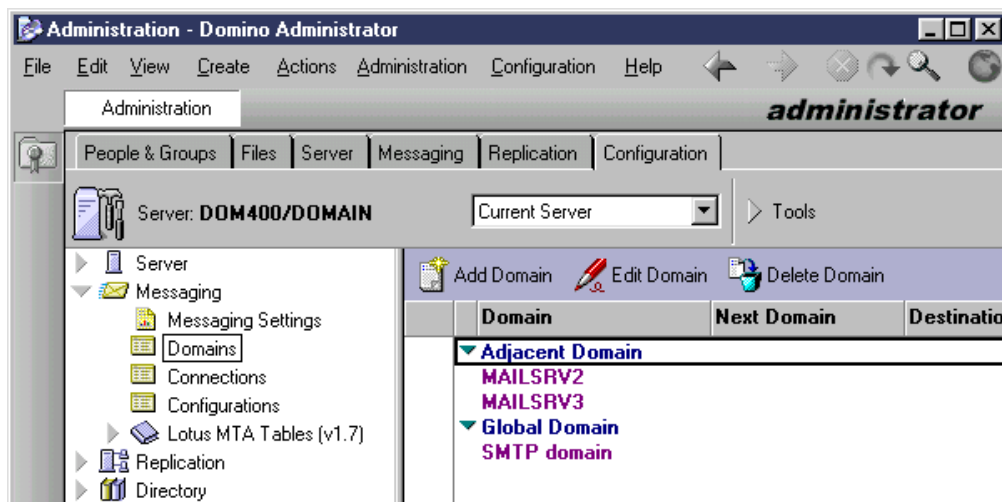


Figure 306. Domain documents

You have now created the two domain documents on DOM400. Repeat these steps for DOMINO2 and DOMINO3.

6.7.3 Creating connection documents

This section describes how to create connection documents. Connection documents allow a Domino server to communicate with other Domino servers on different Domino domains. Refer to Table 30 on page 223 for the configuration values.

Each connection document describes a one-way route to the Domino server located on a different Domino domain. An active connection between two Domino servers is composed of two connection documents, one in each server.

Complete the following steps to create connection documents. On the Domino administrator desktop, refer to Figure 307 for the first five steps.

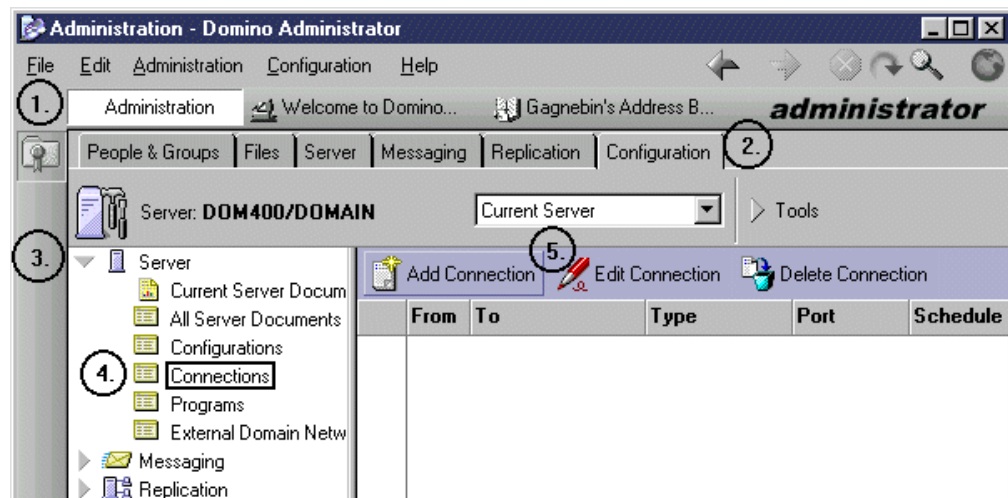


Figure 307. New connection document

1. Click the **Administration** button (1).
2. Click the **Configuration** tab (2).
3. Click **Server** in the navigation tree (3).
4. Click **Connections** (4).
5. Click the **Add Connection** button (5). The display shown in Figure 308 on page 232 appears.

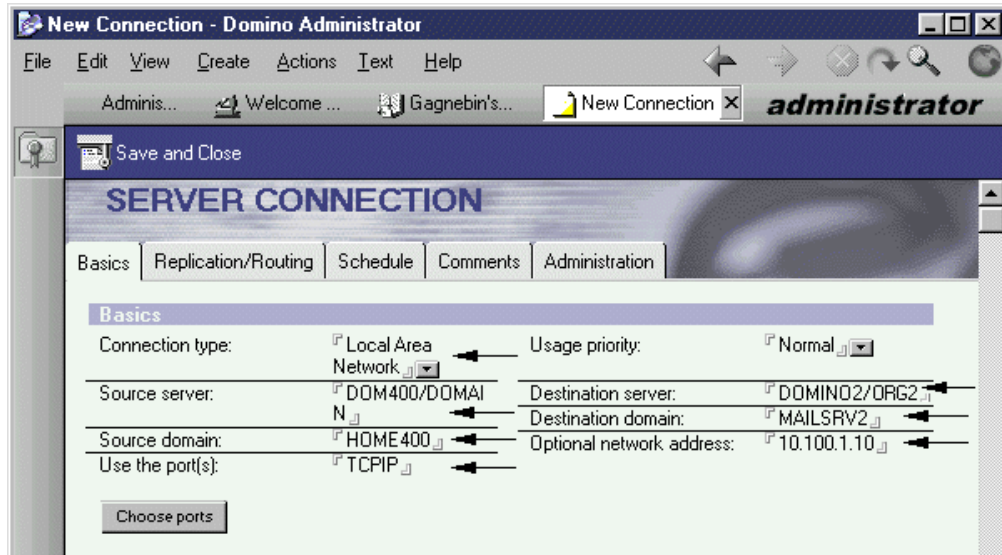


Figure 308. Connection document - Basics

6. Choose the connection type.
7. Enter `DOM400/DOMAIN` for Source server.
8. Enter `HOME400` for Source domain.
9. Enter `TCPIP` for the port used.
10. Enter `DOMINO2/ORG2` for Destination server.
11. Enter `MAILSRV2` for Destination domain.
12. Enter the IP address of your destination server.
13. Click the **Replication/Routing** tab. The display shown in Figure 309 appears.

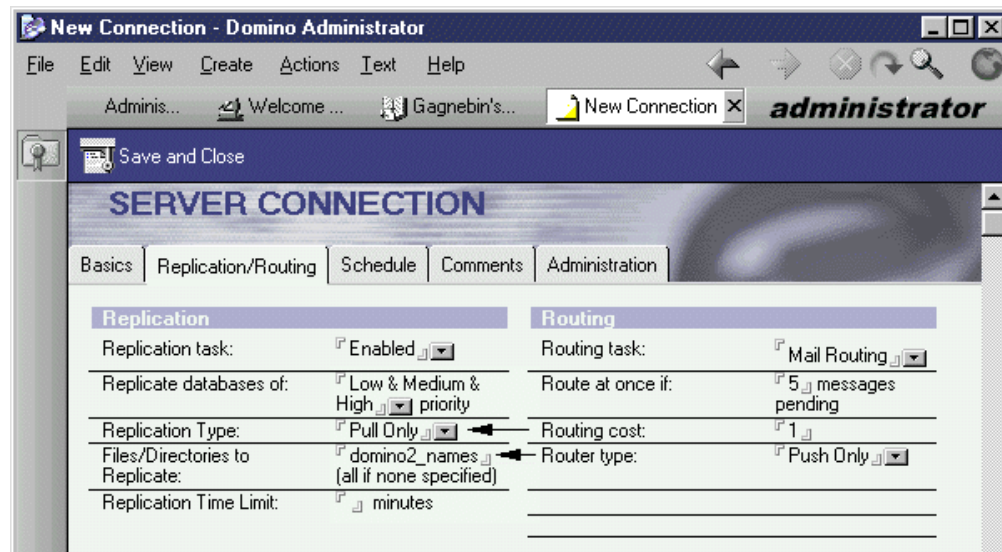


Figure 309. Connection document - Replication/Routing

14. Choose **Pull Only** for Replication type. If you specify Push Pull, you need additional authority on the Public Address Book you want to replicate.

15. Enter `domino2_names` for the file to replicate.
16. Choose the number of queuing messages that are waiting.
17. Click the **Schedule** tab. The display shown in Figure 310 appears.

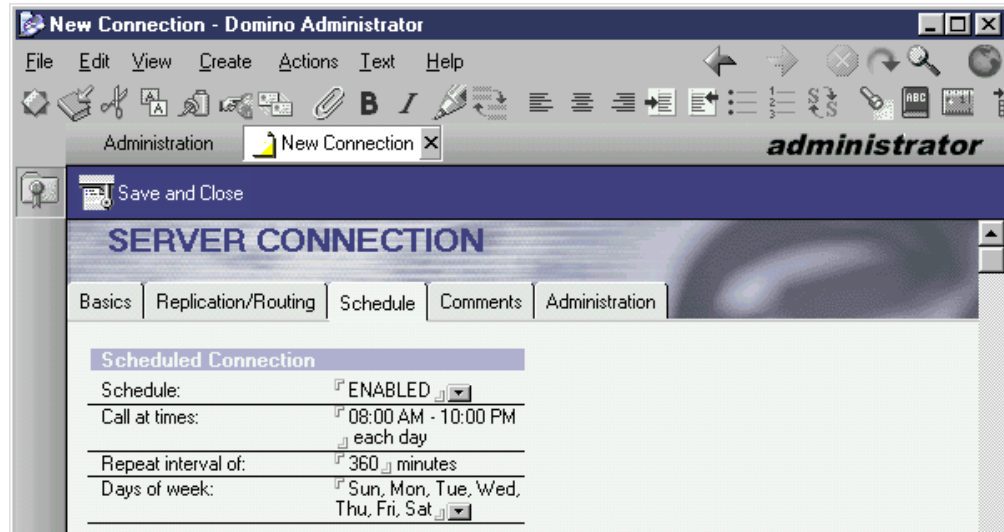


Figure 310. Connection document - Schedule

18. Verify that the schedule parameters match your needs.
19. Click **Save and Close**.

You have created the connection document, and the link from DOM400 to DOMINO2 is created. Now we create a new link from DOM400 to DOMINO3. Follow these steps:

1. Click the **Add Connection** button. The display shown in Figure 311 appears.

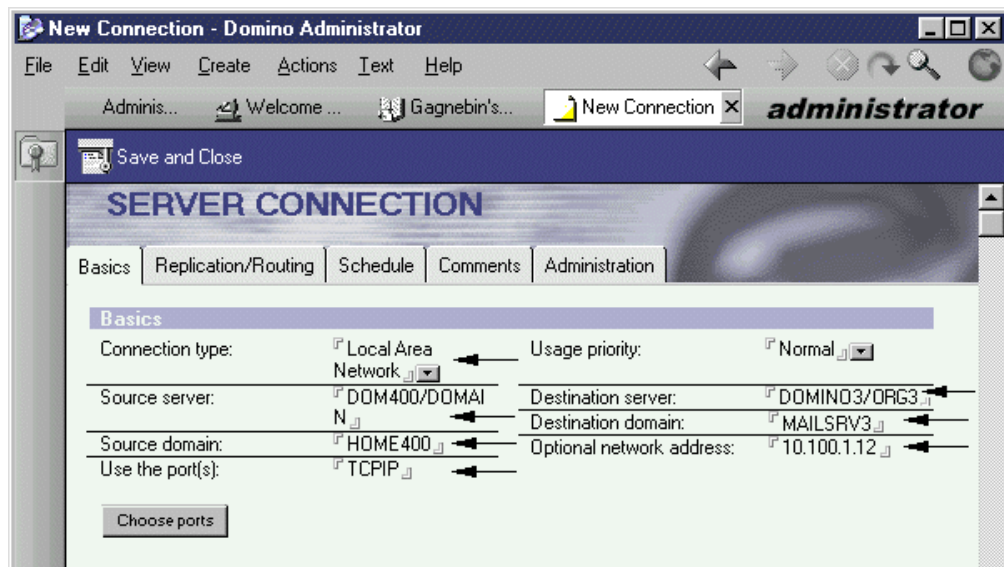


Figure 311. Connection document - Basics

2. Choose the connection type.

3. Enter `DOM400/DOMAIN` for Source server.
4. Enter `HOME400` for Source domain.
5. Enter `TCPIP` as the port used.
6. Enter `DOMINO3/ORG3` for Destination server.
7. Enter `MAILSRV3` for Destination domain.
8. Enter the IP address of your destination server.
9. Click the **Replication/Routing** tab. The display shown in Figure 312 appears.

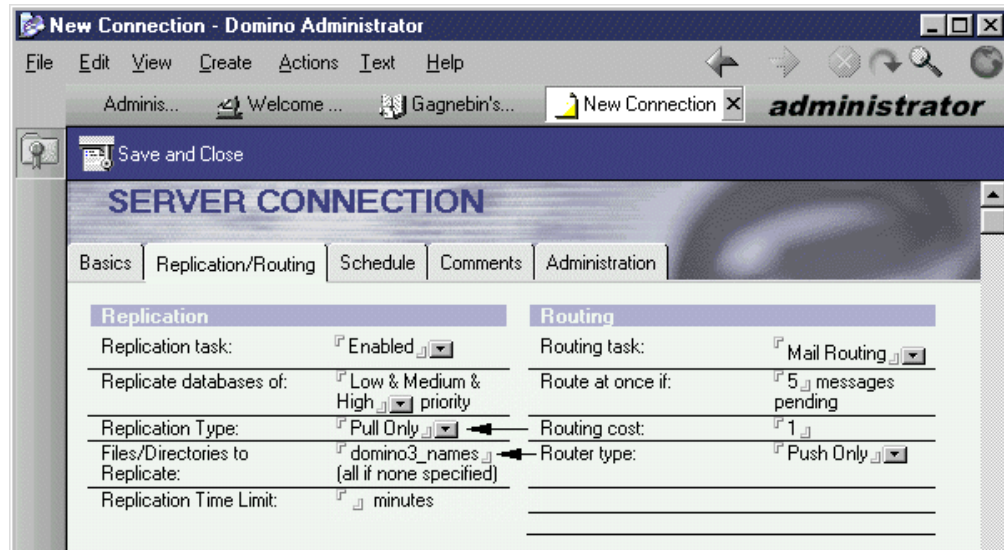


Figure 312. Connection document - Replication/Routing

10. Choose **Pull Only** for Replication Type. If you specify Push Pull, you need additional authority on the Public Address Book you want to replicate.
11. Enter `domino3_names` for the file to replicate.
12. Choose the number of queuing messages that are waiting.
13. Click the **Schedule** tab. The display shown in Figure 313 on page 235 appears.

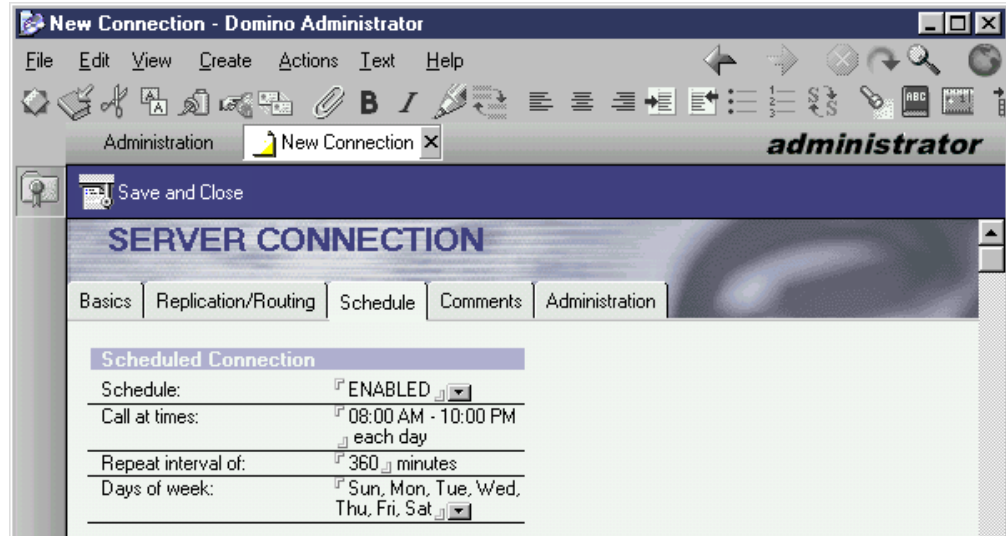


Figure 313. Connection document - Schedule

14. Verify that the Schedule parameters match your needs.
15. Click **Save and Close**. The display shown in Figure 314 appears.

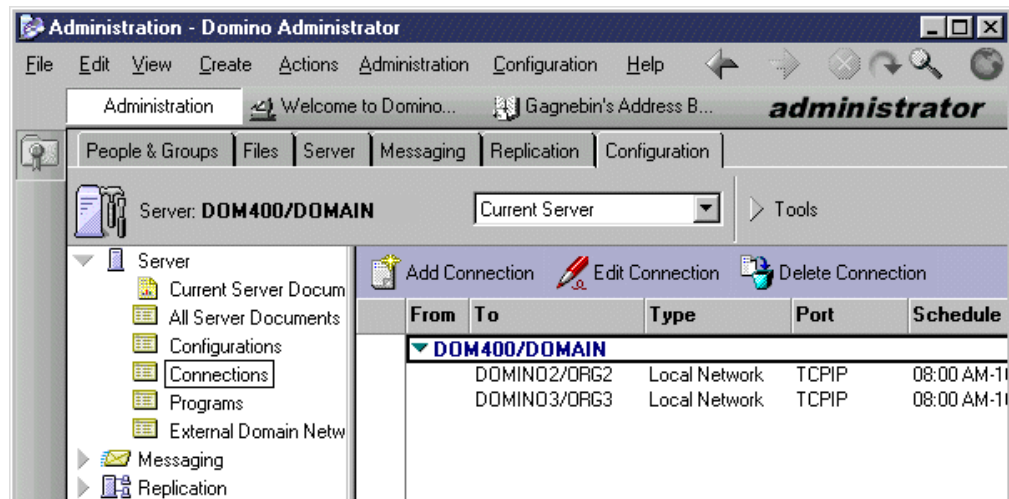


Figure 314. Connection documents

You successfully created the two connection documents on DOM400. Repeat these steps for DOMINO2 and DOMINO3.

After you create all the connection documents on all the servers, you should have two connection documents on each system. DOM400 will have DOMINO2/ORG2 and DOMINO3/ORG3. DOMINO2 will have DOM400/DOMAIN and DOMINO3/ORG3. DOMINO3 will have DOM400/DOMAIN and DOMINO2/ORG2.

6.7.4 Cross certifying the Domino servers

In this section, we cross certify each Domino server with both partners. This gives the authority to replicate the Public Address Book of each Domino domain. Refer to Table 30 on page 223 for the configuration values. On the Domino administrator desktop, refer to Figure 315 on page 236 for steps one through five.

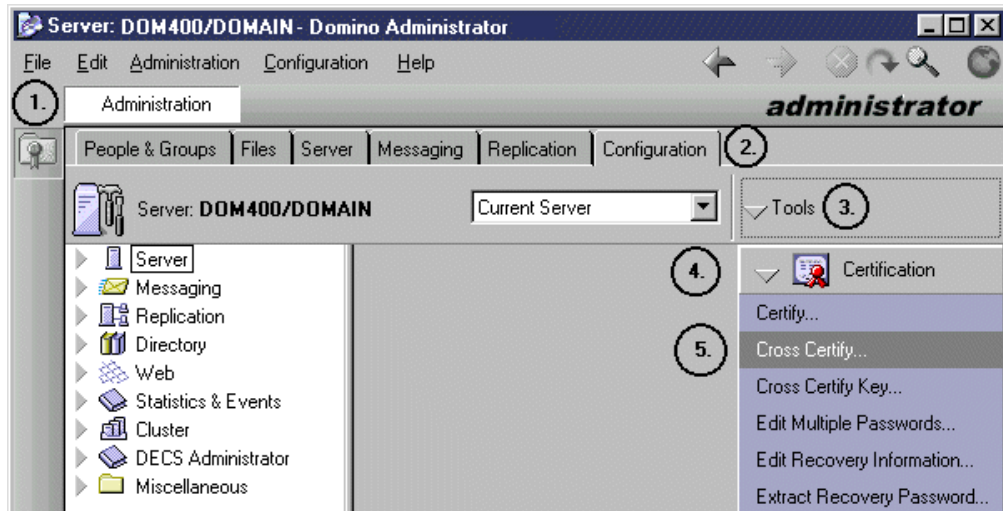


Figure 315. Cross certify - Certification pull-down menu

1. Click the **Administration** button (1).
2. Click the **Configuration** tab (2).
3. Click the **Tools** button (3).
4. Click the **Certification** pull-down menu (4).
5. Click **Cross Certify** (5). The display shown in Figure 316 appears.

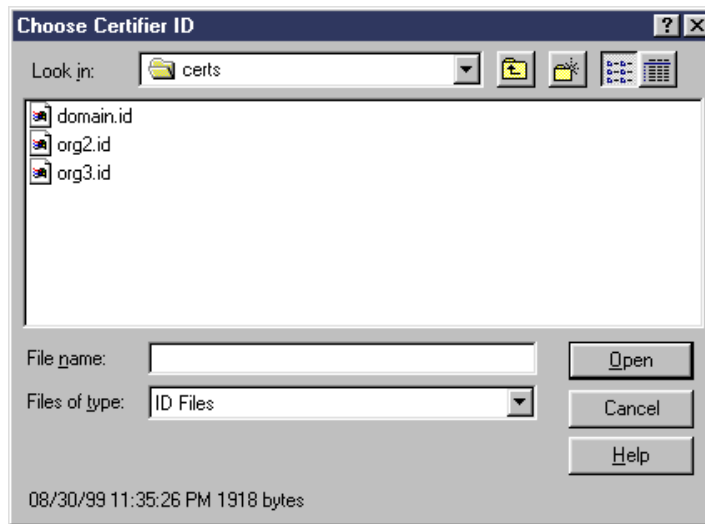


Figure 316. Choose Certifier ID

6. Choose the source cross certifier `domain.id`.
7. Click **Open**. The display shown in Figure 317 on page 237 appears.

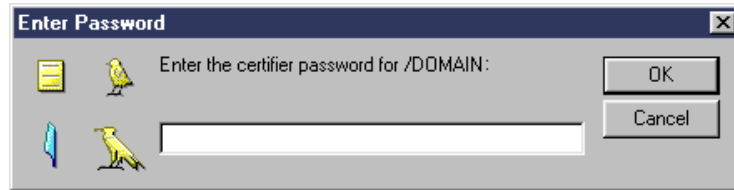


Figure 317. Entering a certifier password

8. Enter the certifier password. The display shown in Figure 318 appears.

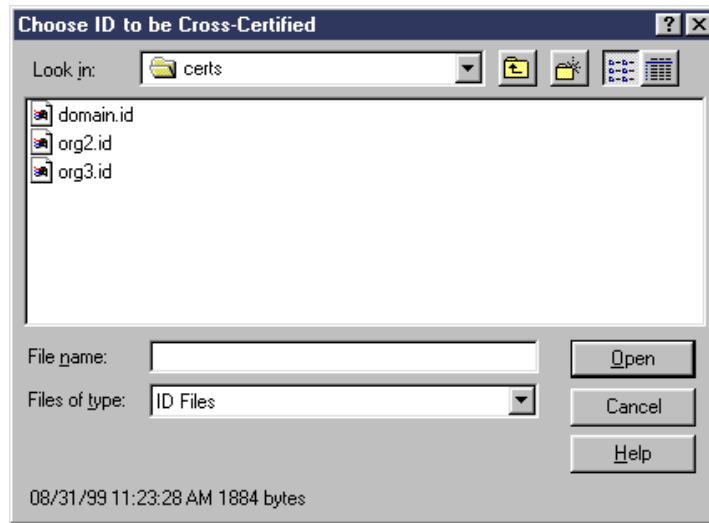


Figure 318. Choose ID to be Cross-Certified

9. Choose the first destination cross certifier `org2.id`.

10. Click **Open**. The display shown in Figure 319 appears.

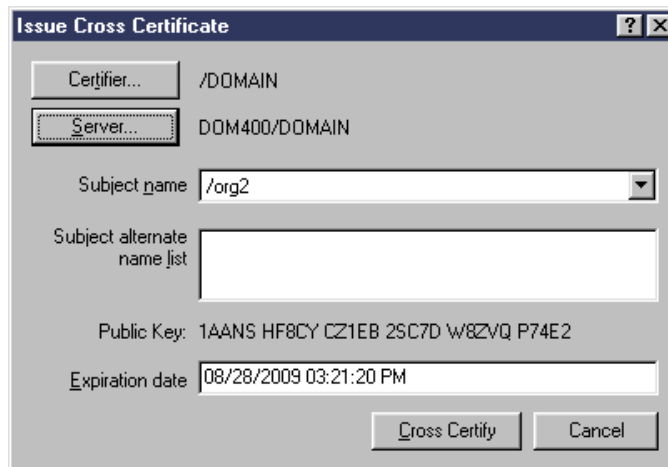


Figure 319. Issue Cross Certificate

11. Verify that Server is the source certifier server.

12. Click **Cross Certify**. The display shown in Figure 320 on page 238 appears.

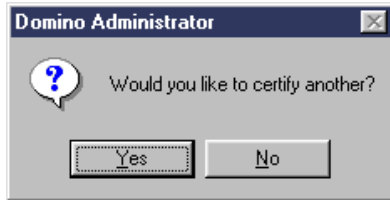


Figure 320. Cross certifying another organization

13. Click **Yes**. The display shown in Figure 321 appears.

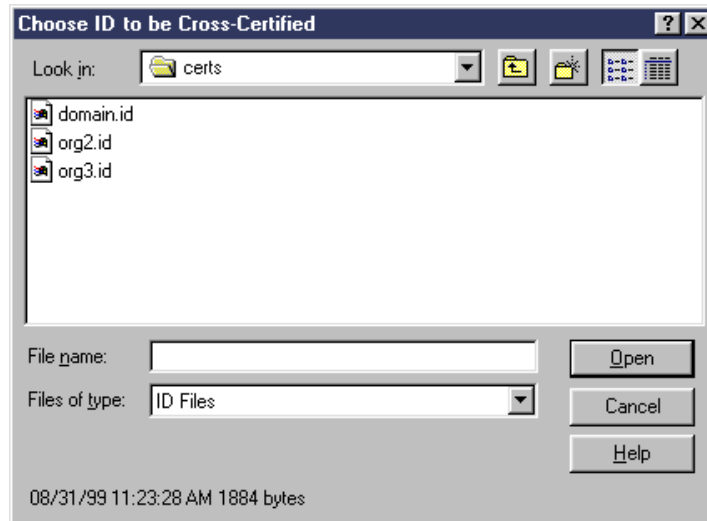


Figure 321. Choose ID to be Cross-Certified

14. Choose the second destination cross certifier `org3.id`.

15. Click **Open**. The display shown in Figure 322 appears.

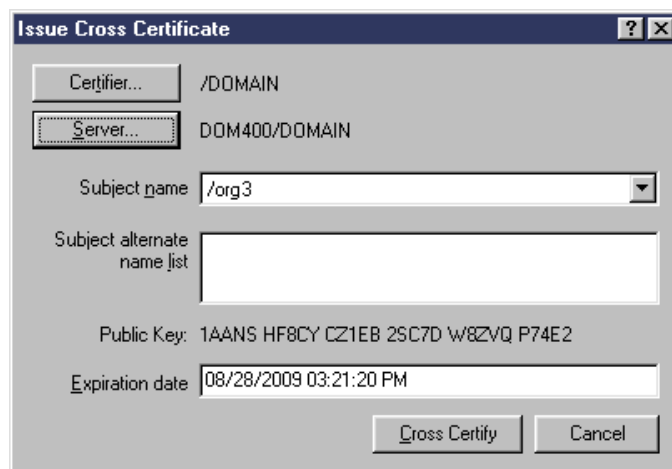


Figure 322. Issue Cross Certificate

16. Verify that Server is the source certifier server.

17. Click **Cross Certify**. The display shown in Figure 323 on page 239 appears.

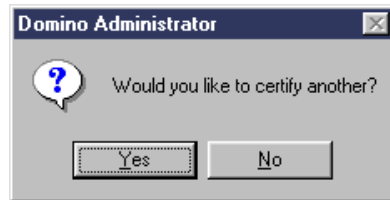


Figure 323. Cross certifying another organization

18. Click **No**. The display shown in Figure 324 appears.

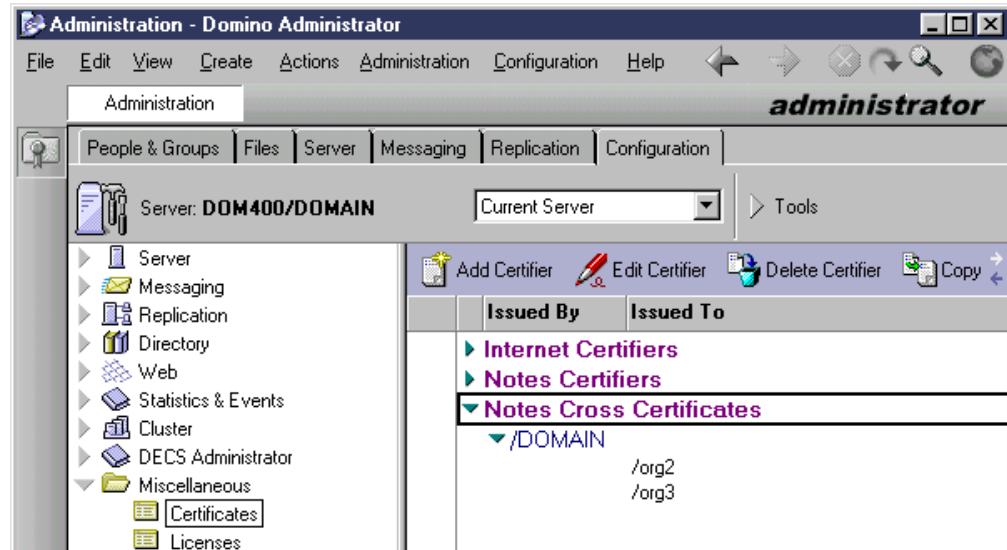


Figure 324. Notes Cross Certificates

Your server DOM400 is now cross certified with the two other servers. Repeat these steps for DOMINO2 and DOMINO3.

6.8 Configuring replications

This section describes the tasks that you must perform to configure the replication process for each Public Address Book. The replication is pull only (read only). It means that the partner servers are only allowed to read (not to modify) the Public Address Book in the source server (domain). This a good security feature.

The Domino servers DOM400, DOMINO2, and DOMINO3 have the same configuration. We use Domino server *DOM400* as a reference. Please follow the instructions in this section and refer to Table 30 on page 223 for the configuration values.

6.8.1 Task summary

The following list summarizes the tasks used to configure the replications on the three Domino servers:

1. Give replication authority to the Domino servers.
2. Set up replication.
3. Enable Public Address Book Lookup.

6.8.2 Giving replication authority to the Domino servers

In this section, we give replication authority to both Domino partners. This allows the Domino server to replicate the Public Address Book of its two partners. Refer to Table 30 on page 223 for the configuration values.

Complete the following steps to create domain documents. On the Domino Administrator desktop, refer to Figure 325 for steps one through five.

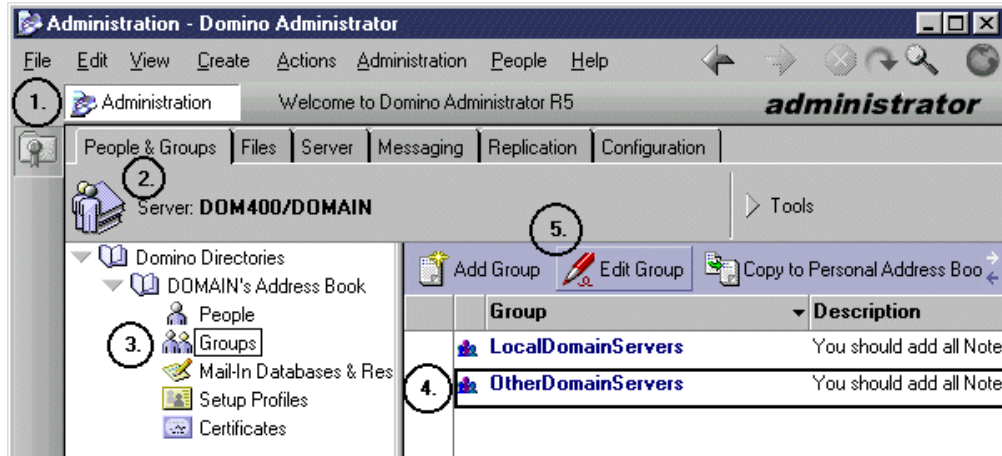


Figure 325. Selecting the group *OtherDomainServers*

1. Click the **Administration** button (1).
2. Click the **People & Groups** tab (2).
3. Click **Groups** in the navigation tree (3).
4. Select **OtherDomainServers** group (4).
5. Click the **Edit Group** button (5). The display shown in Figure 326 appears.

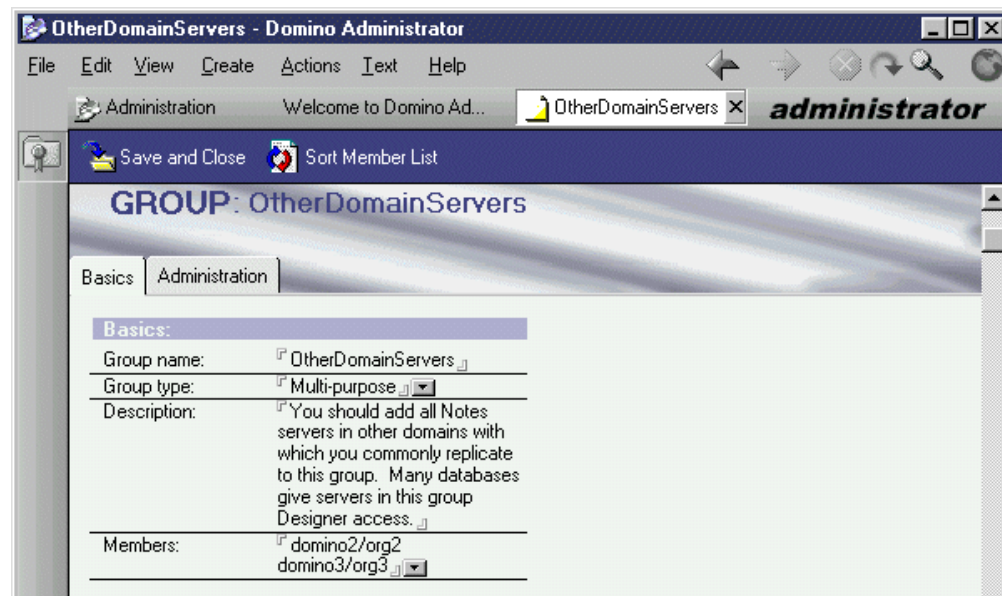


Figure 326. Group *OtherDomainServer* - Basics

6. Enter **DOMINO2/ORG2** and **DOMINO3/ORG3** as members.
7. Click **Save and Close**.

You have now added DOMINO2 and DOMINO3 as members of OtherDomainServers. Next, we modify the server document to give replication authority to this server. Refer to Figure 327 for steps one through four.

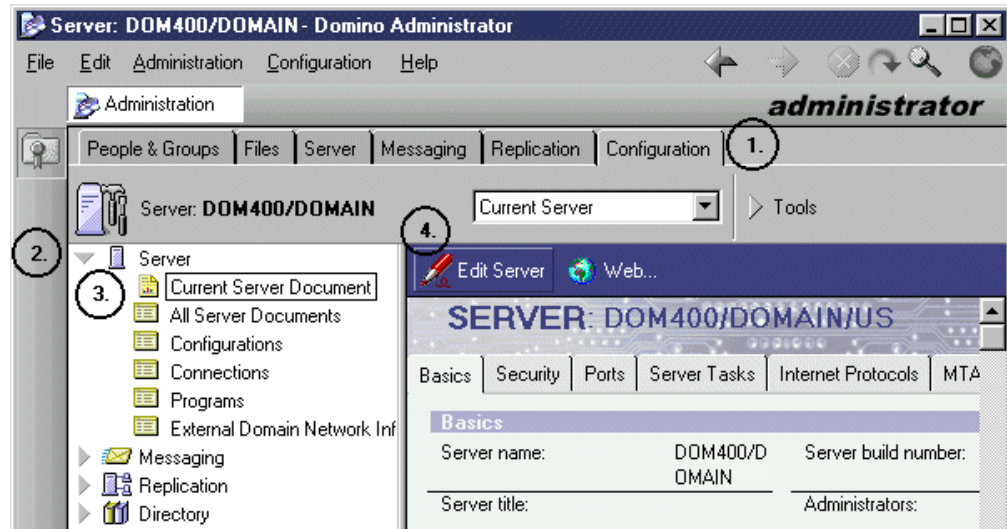


Figure 327. Server document

1. Click the **Configuration** tab (1).
2. Click **Server** in the navigation tree (2).
3. Select the **OtherDomainServers** group (3).
4. Click the **Edit Server** button (4). The display shown in Figure 328 appears.

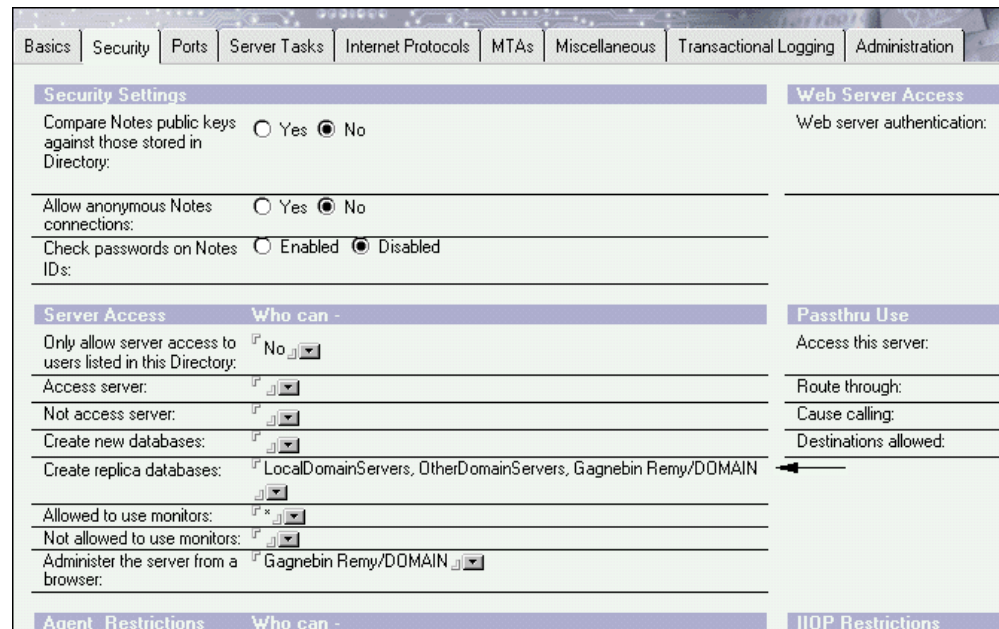


Figure 328. Server document - Security

5. Enter LocalDomainServers, OtherDomainServers, and the administrator in the Create replica databases field.
6. Click **Save and Close**.

You have now successfully given replication authority on DOM400 for the DOMINO2 and DOMINO3 servers. Repeat these steps for DOMINO2 and DOMINO3.

6.8.3 Setting up replications

In this section, we set up the replication for both Domino Public Address Book partners. The source Domino server replicates the Public Address Book of its two partners. This is a pull replication.

For the replication type, refer to Figure 309 on page 232 and Figure 312 on page 234.

For the Public Address Book name (database name), refer to Figure 308 on page 232 and Figure 311 on page 233.

Refer to Table 30 on page 223 for the configuration values.

Complete the following steps to set up the replications. Refer to Figure 329 for steps one and two.

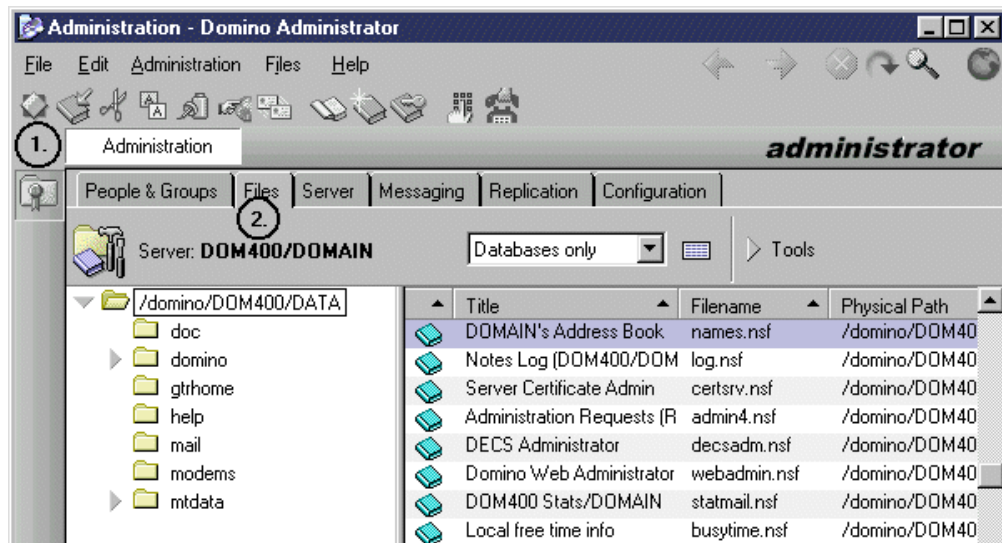


Figure 329. Replication

1. Click the **Administration** button (1).
2. Click the **Files** tab (2).
3. Open the **File** menu. Select **Replication**, and then select **New Replica**. The display shown in Figure 330 on page 243 appears.

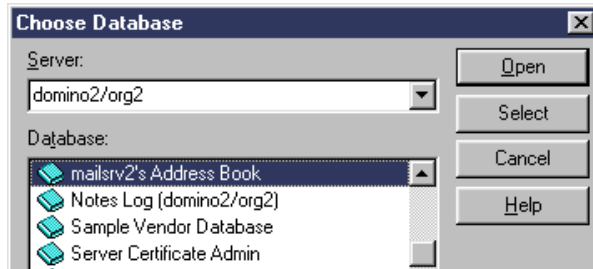


Figure 330. Replication - Choose Database

4. Select **domino2/org2** (source replication server) in the server pull-down menu.
5. Select the Public Address Book of the source server.
6. Click **Open**. The display shown in Figure 331 appears.

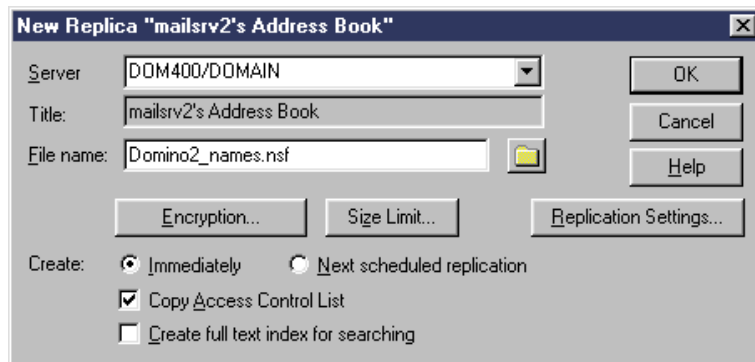


Figure 331. Replication - New Replica "mailsrv2's Address Book"

7. Select **DOM400/DOMAIN** (destination replication server) in the server pull-down menu.
8. Enter `Domino2_names.nsf` for the destination file name.
9. Choose **Immediately** for create.
10. Click **OK**. The display shown in Figure 329 on page 242 appears.

You now have created the replication for the Public Address Book of DOMINO2. Next, we create a new the replication for the Public Address Book of DOMINO3. Continue with the following steps:

11. Open the **File** menu. Select **Replication** and then **New Replica**. The display shown in Figure 332 appears.

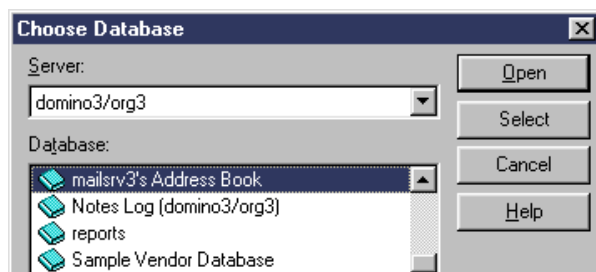


Figure 332. Replication - Choose Database

12. Select **domino3/org3** (source replication server) in the server pull-down menu.
13. Select the Public Address Book of the source server.
14. Click **Open**. The display shown in Figure 333 appears.

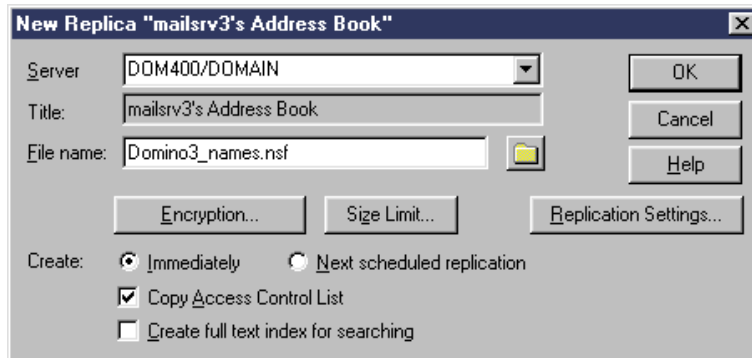


Figure 333. Replication - New Replica "mailsrv3's Address Book"

15. Select **DOM400/DOMAIN** (destination replication server) in the server pull-down menu.
16. Enter `Domino2_names.nsf` for the destination file name.
17. Choose **Immediately** for Create.
18. Click **OK**. The replication process can take several minutes.
19. Verify that the two Public Address Books are created as shown in Figure 334.

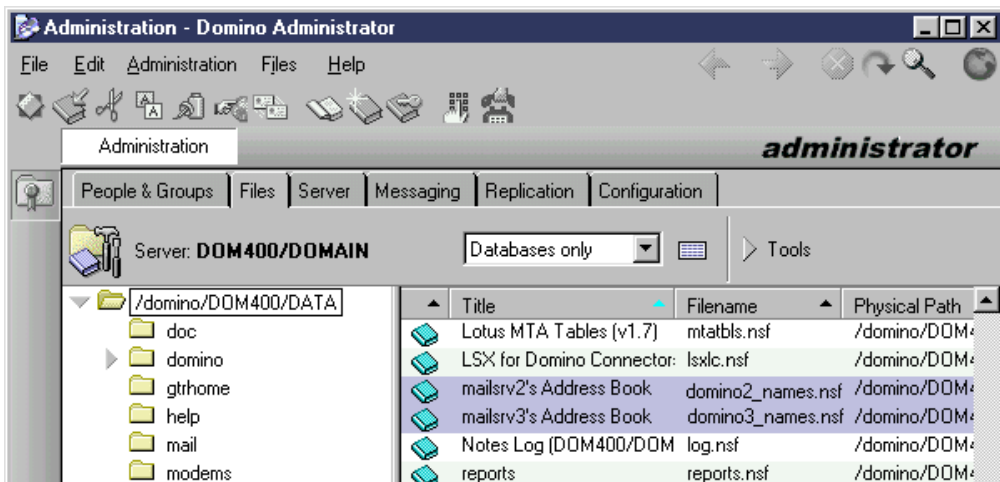


Figure 334. Replication - Result

You now created the replication for the Public Address Book of DOMINO2 and DOMINO3 on the DOM400 server. Repeat these steps on the DOMINO2 and DOMINO3 servers.

6.8.4 Enabling Public Address Book lookup

In this section, we enable each Domino server to look up the two Public Address Book partners (the databases that have been replicated). By default, the Domino

server performs a lookup only in its own Public Address. Refer to Table 30 on page 223 for the configuration values.

Complete the following steps to enable lookup in more than one Public Address Book:

1. On an AS/400 command line, type:

```
WRKDOMSVR
```

The screen shown in Figure 335 appears.

```
                                Work with Domino Servers                                System:  HOME400
Type options, press Enter.
 1=Start server   2=Change server   5=Display console  6=End server
 7=Submit command 8=Work console   9=Work server jobs
11=Change current directory 12=Work object links 13=Edit NOTES.INI

      Domino                               Domino
Opt  Server                               Subsystem  Status
13  DOM400                               DOMINO01   *STARTED
```

Figure 335. Work with Domino Servers

2. Type 13, and then press Enter.
3. Press the Page Down key until you reach the end of the file (Figure 336).

```
Edit File: /DOMINO/DOM400/DATA/NOTES.INI
Record . :      82 of      90 by      8          Column:      1 of      59 by      74
Control  :

CMD .....1.....2.....3.....4.....5.....6.....7.....+
TRANSLOG_UseAll=0
TRANSLOG_Style=0
TRANSLOG_Performance=2
TRANSLOG_Status=0
MTEEnabled=1
WebAdminSetup=5
DominoConfigLevel=3
I  SCHEDULE_VERSION=3
*****End of Data*****
```

Figure 336. Edit Notes.ini (Part 1 of 2)

4. Type I (insertion) beside the last line.
 5. Type NAMES=NAMES, DOMINO2_NAMES, DOMINO3_NAMES. Press Enter.
- The Notes.ini file should appear as shown in Figure 337 on page 246.

```

Edit File: /DOMINO/DOM400/DATA/NOTES.INI
Record . :      82 of      90 by      8          Column:      1 of      59 by      74
Control  :

CMD .....1.....2.....3.....4.....5.....6.....7.....+
TRANSLOG_UseAll=0
TRANSLOG_Style=0
TRANSLOG_Performance=2
TRANSLOG_Status=0
MTEEnabled=1
WebAdminSetup=5
DominoConfigLevel=3
SCHEDULE_VERSION=3
NAMES=NAMES,DOMINO2_NAMES,DOMINO3_NAMES
*****End of Data*****

```

Figure 337. Edit Notes.ini (Part 2 of 2)

6. Restart your server so the changes can take effect.

You now modified the notes.ini of DOM400 server. Repeat these steps for DOMINO2 and DOMINO3.

The setup of your three Domino servers is completed. You can now send e-mail from the Internet to each Domino server through DOM400.

6.9 Creating Lotus Notes mail users

The Domino server is now ready to receive mail from the Internet. In this section, we create a Lotus Domino user and their mailbox. Refer to Table 30 on page 223 for the configuration values. Complete the following steps. Refer to Figure 338 for steps one through five.

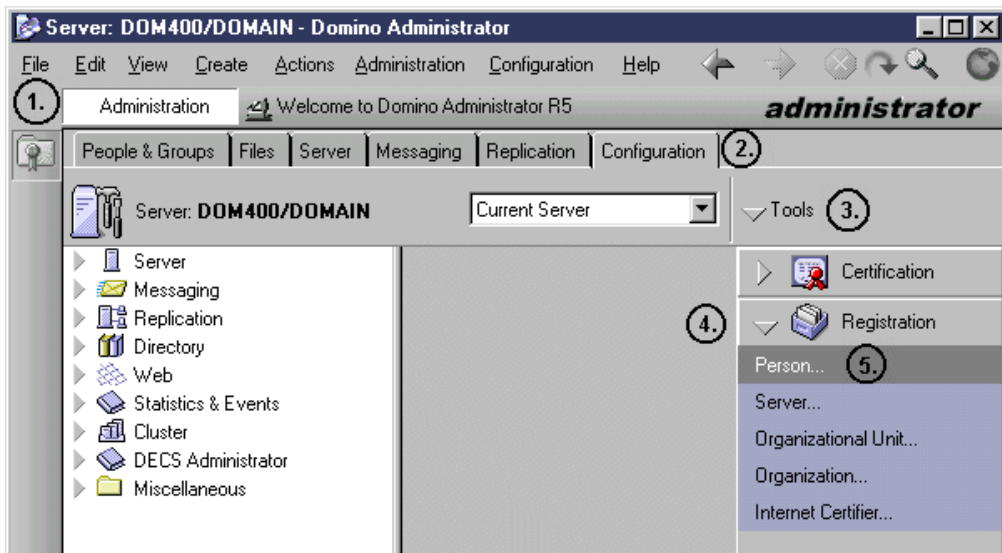


Figure 338. Registration - Person

1. On the Domino Administrator desktop, click **Administration** (1).
2. Click the **Configuration** tab (2).

3. Click the **Tools** pull-down menu (3).
4. Click **Registration** (4).
5. Click **Person** (5). The display shown in Figure 339 appears.

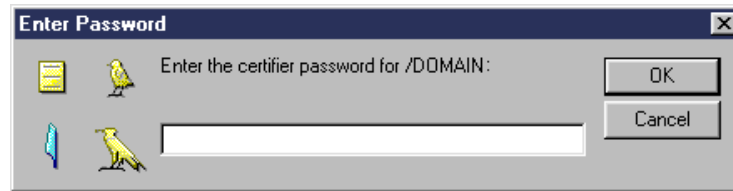


Figure 339. Certifier ID password

6. Enter the password, and then click **OK**. The display shown in Figure 340 appears.

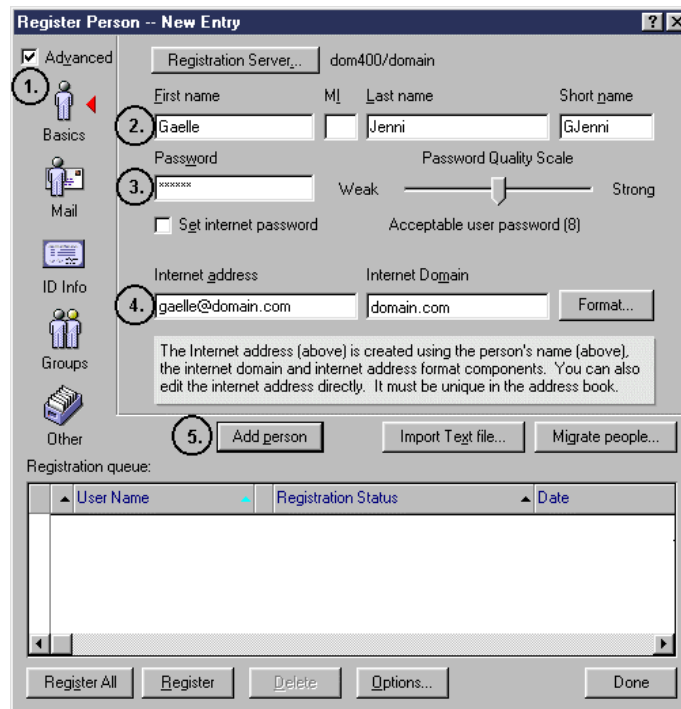


Figure 340. Register Person (Part 1 of 2)

7. Check **Advanced**.
8. Enter the person's first name and last name.
9. Enter the person's password.
10. Enter the person's Internet address and Internet domain.
11. Click the **Add person** button. The display shown in Figure 341 on page 248 appears.

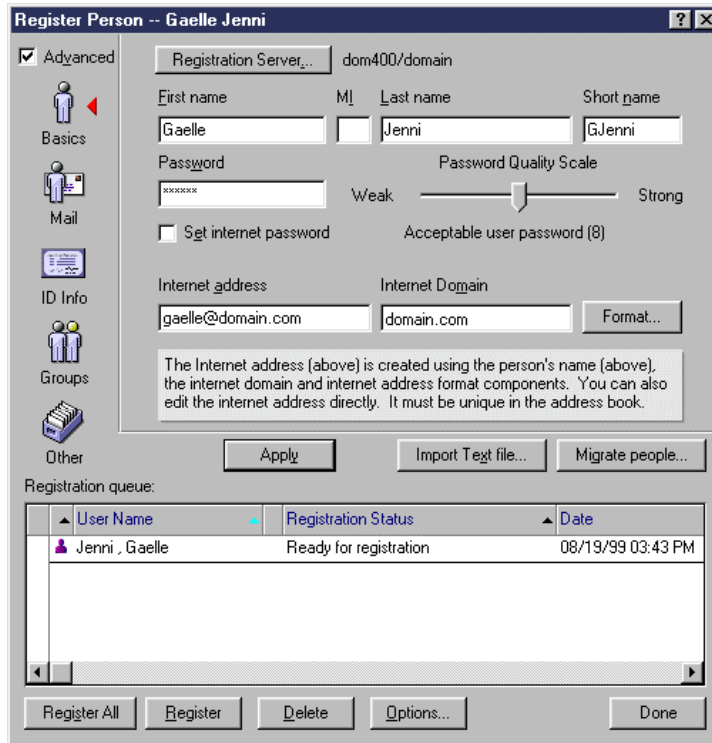


Figure 341. Register Person (Part 2 of 2)

12. Click the **Register** button.

The registration process can take several minutes.

You now successfully registered your user and mailbox. The user ID is stored on the DOM400 Public Address Book. Repeat these steps for a different user on DOMINO2 and DOMINO3.

The last step is to configure Lotus Notes on your PCs. If you never before configured Lotus Notes for your mail, refer to the Lotus documentation that came with the product.

Chapter 7. Problem determination

This chapter provides basic problem determination information. For detailed problem determination information, refer to the product documentation. The redbook *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162, has a complete chapter about problem determination. That information will not be repeated here. For additional information about problem determination, refer to *IBM Firewall for AS/400 V4R3: VPN and NAT Support*, SG24-5376.

7.1 IBM Firewall for AS/400

This section provides conditions that can interfere with access to the Internet by a client behind the firewall using NAT. If you cannot access a public server behind the firewall, check these items:

- Make sure that IP forwarding is permitted.
- Make sure that the NAT server is started.
- Make sure that the filter rules are correct.
- Make sure the router to the ISP is configured correctly. If *publicAddress* of the NAT MAP setting is the same as the firewall's non-secure IP address, no additional routes are required. If *publicAddress* is some other address, the router must be configured so that it routes traffic destined for *publicAddress* through the non-secure IP address of the firewall.
- Make sure port mapping is only used with the TCP protocol.
- Port mapping is used when you use different *From_port* and *To_port* values. It only works when you use the TCP protocol. Do not use port mapping with other protocols such as UDP.
- NAT does not support ping. You cannot use the ICMP protocol with NAT. This includes not being able to ping through the firewall using NAT.

CWBPing

If you have a PC with Client Access Express for Windows V4R4 installed on the non-secure side of the network, you can test NAT by using this command in the DOS shell:

```
CWBPING 208.222.150.250 /Port:110
```

If the response is negative, it means that NAT is not working properly.

- Make sure that you added the default route in OS/400 to point to the *INTERNAL port of the firewall (192.168.2.2 in our example) if you are running a public server in the same AS/400 system that houses the firewall.
- Enable logging on each of the NAT filtering rules to assist in tracing the packet flow. Changing the firewall logging level to **i** (informational) while debugging a problem is also recommended. During normal operation of the firewall, set logging level to **w** (warning).
- When viewing the firewall logs, it is helpful to click **Bottom**, which takes you to the last page of the log and refreshes it at the same time.

Remember

Any time you change a filter rule, you *must* restart filtering. If you allow logging as suggested, you must restart filtering to see the additional log entries.

For more information about problem determination, refer to *AS/400 Internet Security: IBM Firewall for AS/400, SG24-2162*, and *IBM Firewall for AS/400 V4R3: VPN and NAT Support, SG24-5376*.

7.2 IBM eNetwork Firewall for Windows NT

This section provides conditions that can interfere with access to the Internet by a client behind the firewall using NAT. If you cannot access a public server behind the firewall, check these items:

- Make sure that NAT has been activated.
- If the NAT address is in the same subnet, make sure you added the IP addresses to the alias on the Windows NT system.
- Make sure that the filter rules are correct.
- NAT does not support ping. You cannot use the ICMP protocol with NAT. This includes not being able to ping through the firewall using NAT.

CWBPing

If you have a PC with Client Access Express for Windows V4R4 installed on the non-secure side of the network, you can test NAT by using this command in the DOS shell:

```
CWBPING 208.222.150.251 /Port:110
```

If the response is negative, it means that NAT is not working properly.

- Make sure you added the default route in OS/400 to point to the secure port of the firewall (10.100.1.7 in our example) if you are running a public server in the same AS/400 system that houses the firewall.
- Enable logging in each rule to assist in tracing the packet flow. Changing the firewall logging level to debug is also recommended. During normal operation of the firewall, set the logging level to warning.
- When viewing the firewall logs, it is helpful to click **Bottom**, which takes you to the last page of the log and refreshes it at the same time.

Remember

Any time you change a filter rule, you *must* regenerate *Connection Rules and Activate*. If you allow logging as suggested, you must restart filtering to see the additional log entries.

For more information about problem determination, refer to *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT, SG24-5209*.

7.3 AS/400 e-mail problem determination

E-mail troubleshooting needs to be broken into parts. Determination needs to be made regarding whether the issue involves the SMTP servers, Domain Name System Server (DNS), firewall, or the network.

Because the AS/400 system is such a versatile e-mail server and supports so many different kinds of e-mail, including SMTP/POP, OS/400 - TCP/IP and SNA, Lotus Domino - TCP/IP, and Notes Remote Procedure Call (NRPC), take extra care in evaluating the status of the internal workings of the AS/400 system, including:

- SMTP server for inbound mail
- SMTP client for outbound mail
- Mail Server Framework
- OS/400 Resolver
- System Distribution Directory
- SMTP server attributes
- POP server attributes

Also, with the release of Lotus Domino Server Version 5.0, two separate Domino configurations are possible. The first configuration consists of using the Domino Router, OS/400 SMTP Servers, the OS/400 Mail Server Framework, and the OS/400 Resolver and TCP/IP Stack. The second configuration consists of using the Domino Router, Domino's SMTP Server Function, and the OS/400 Resolver and TCP/IP Stack.

Whether *MSF or *DOMINO was selected as the SMTP method during configuration of the Domino Server on the AS/400 system dictates how e-mail troubleshooting is performed on the AS/400 system and Domino.

7.4 OS/400 SMTP and Lotus Domino R5 configured *MSF

Certain tools can be used to obtain data that is useful for troubleshooting the various components of OS/400 and Domino. These include:

- Communications trace
- SMTP flow
- MSF mail flow
- Domino message tracking

7.4.1 Outbound or Inbound mail flow on the AS/400 interface

To determine whether mail is flowing inbound or outbound on the AS/400 Interface that connects to the intranet or Internet, a communications trace is required. The configuration of your AS/400 system, and whether the Integrated PC Server is configured as a LAN adapter, determines whether a communications trace of the line or a communications trace of the network server description is required.

7.4.1.1 DNS traffic

Before e-mail can be sent to another mail server, the recipient's SMTP domain must be found on the Internet. The resolver of the sending e-mail server must query DNS to determine where to send the e-mail. Normally, the resolver first attempts to make a connection with the DNS server using User Datagram

Protocol (UDP). If a connection can't be made to the DNS Server with UDP, the resolver of the sending mail server attempts to contact the DNS server using TCP.

Typically, most of the DNS traffic uses UDP. If TCP is used, an issue may exist with connectivity to the DNS server.

7.4.1.2 SMTP traffic

If the sending mail server's resolver successfully obtains the mail server that is handling mail for the domain of the recipient, the sending SMTP server attempts to open a connection to the remote (receiving) SMTP server on Port 25. The usual TCP connectivity of SYN, SYN ACK, or ACK will take place.

7.4.2 Pre-V4R4 Flight Recorders and the V4R4 Flight Recorders

The SMTP Flight Recorders are valuable for determining whether the OS/400 SMTP server is accepting mail or the SMTP client is sending mail. The steps that the SMTP server uses to obtain name resolution can be monitored. The path of queries to both the local host table and to the DNS servers can be traced. Use the SMTP Flight Recorders when additional information is needed besides the communication trace.

7.4.3 Mail flow through the Mail Server Framework (MSF)

MSF handles the transfer of mail flow between the OS/400 SMTP Servers and the AS/400 Native Domino Server. Various snap-ins or User Exit Points can be plugged into the Mail Server Framework. The key to remember about MSF is that MSF only acts as a director of mail. MSF only processes pointers to pieces of mail. Because each pointer is processed by the MSF, a method is required to actually see the mail pointer traverse the exit points from the top of MSF to the bottom of MSF. To determine if or where a mail issue exists in the MSF, the AnyMail Dump snap-in can be used.

7.4.4 Tracking mail through SMTP, MSF, and internal AS/400 objects

A new capability of the AS/400 system is the ability to track mail through the system using Component Journaling. At this time, Component Journaling allows the tracking of mail up to the Domino Server. The Domino Server does not use Component Journaling. Only OS/400 Native Servers make use of the Component Journaling. One major benefit of Component Journaling is the ability to monitor the OS/400 Resolver, because both the *DOMINO and *MSF Domino servers use the OS/400 Resolver. The Journaling Point named *8K MX Resol* can be used to determine issues with name resolution.

Component Journaling helps you understand how mail flows through the major components and lists the reasons why your mail may not be delivered. There are various queues and programs used by the mail delivery and server functions. The intent of the journaling function is to document the following items:

- Transitions
 - Programs to queues
 - Queues to programs

- Events
 - Arrival of mail via the server
 - Delivery of mail via the client
 - Storage of mail on retry queues or resource busy queues
- Tracking and some measurement data
 - 822 Message ID
 - MSF Message ID
 - Size of message
 - Originator
 - Recipients

7.4.5 Monitoring mail using Domino Message Tracking

Both Domino administrators and end users can track mail within Domino using Domino Message Tracking. Administrators can track mail sent by any user, while end users can track only messages that they themselves sent. Domino records all message-tracking information in the Mail Tracking Store database (MTSTORE.NSF).

7.5 Lotus Domino using native Domino SMTP on the AS/400 system

When Domino for AS/400 is configured with SMTP(*DOMINO), the Lotus Domino SMTP Server Function is installed. In this case, the OS/400 SMTP Servers are not used. Also, MSF is not used. Troubleshooting this scenario requires the use of:

- Communication Trace or Network Server Description (NWSD) Trace
- Domino Message Tracking

7.6 Collecting pre-V4R4 SMTP Flight Recorders

Take care when using the SMTP Flight Recorders. The Flight Recorders must be turned off after the data is collected. If they are left on, the Flight Recorders could fill all of your DASD. Follow these steps:

1. On the OS/400 command line, type:

```
ENDTCPSVR *SMTP
```

Press Enter.

2. Remember to *give the SMTP servers enough time to shut down*. To check them, on the OS/400 command line, type:

```
WRKACTJOB SBS(QSYSWRK)
```

Press Enter.

Server Jobs QTSMTPLNT, QTSMTPSRVR, QTSMTPBRCCL, and QTSMTPBRSR should not be present.

3. On the OS/400 command line, type:

```
CALL QCMD
```

Press Enter.

Note: This starts the command line screen. To exit the command line screen, press the **F12** function key.

4. On the OS/400 command line, type:

```
DLTF FILE(QUSRSYS/QTMSFLRCF*)
```

Press Enter.

5. On the OS/400 command line, type:

```
CRITDTAARA DTAARA(QUSRSYS/QTMSTRCNL) Type(*CHAR) + VALUE('11111100')  
TEXT('SMTP Debug control data area')
```

Press Enter.

6. On the OS/400 command line, type:

```
STRTCPSVR *SMTP
```

Press Enter.

7. Verify that all four SMTP Jobs are active. On the OS/400 command line, type:

```
WRKACTJOBSBS(QSYSWRK)
```

Press Enter.

The following SMTP Server Jobs should be running in QSYSWRK:
QTSMTPLCNT, QTSMTPSRVR, QTSMTPBRCCL, and QTSMTPBRSR.

8. Run the test scenario that is causing the issue.

9. On the OS/400 command line, type:

```
ENDTCPSVR *SMTP
```

Press Enter.

Allow time for SMTP to shut down. Then, type:

```
DLTDTAARA DTAARA(QUSRSYS/QTMSTRCNL)
```

Press Enter.

10. On the OS/400 command line, type:

```
STRTCPSVR *SMTP
```

Press Enter.

11. To view the SMTP Flight Recorders, type the following command on the OS/400 command line:

```
WRKF FILE(QUSRSYS/QTMSFLRCF*)
```

Press Enter (see Table 32).

Table 32. Spooled files generated by the SMTP Flight Recorder

Trace file	Job number	SMTP job
QUSRSYS/QTMSFLRCF0		
QUSRSYS/QTMSFLRCF1	1	QTSMTPLCNT
QUSRSYS/QTMSFLRCF2	2	QTSMTPSRVR
QUSRSYS/QTMSFLRCF3	3	QTSMTPBRCCL
QUSRSYS/QTMSFLRCF4	4	QTSMTPBRSR
QUSRSYS/QTMSFLRCF5		

7.7 Collecting V4R4 Flight Recorders

In V4R4, new SMTP servers were designed, along with a new method of collecting SMTP data. The TRCTCPAPP Tool captures SMTP inbound and outbound connections.

Restrictions

For a given application, only one trace instance can be active at a time. Therefore, for a given application, the command can only be used by one user at a time.

A PTF that is required for the V4R4 Flight Recorders is PTF SF58088 (APAR SA81557, 5769TC1).

7.7.1 TRCTCPAPP parameter settings for e-mail on the AS/400 system

There are two TRCTCPAPP parameter settings for e-mail on the AS/400 system. They are explained in the following sections.

7.7.1.1 *SMTPSVR

The *SMTPSVR parameter specifies tracing for the SMTP server handling inbound mail processing connections.

For SMTP inbound connections (*SMTPSVR), the trace information can be filtered by:

- Remote IP address
- Port
- Recipient mail address

7.7.1.2 *SMTPCLT

The *SMTPCLT parameter specifies tracing for the SMTP client handling outbound mail processing connections.

For SMTP outbound connections (*SMTPCLT), the trace information can be filtered by:

- Recipient host name
- Recipient address
- Mail exchanger information

7.7.2 SMTP inbound connections *SMTPSVR

On the AS/400 command line, type:

```
TRCTCPAPP
```

Then, press **F4** to prompt. The screen shown in Figure 342 on page 256 appears.

```

Trace TCP/IP Application (TRCTCPAPP)

Type choices, press Enter.

TCP/IP application . . . . . > *SMTPSVR      *FTP, *SMTPSVR, *SMTPCLT...
Trace option setting . . . . . *ON          *ON, *OFF, *END, *CHK
Maximum storage for trace . . . *APP_____ 1-16000, *APP
Trace full action . . . . . *WRAP_____ *WRAP, *STOPTRC
Recipient mail address . . . . . _____

-----

Remote network address:
Address family . . . . . _____ *INET
IP address . . . . . _____
Subnet mask . . . . . '255.255.255.255'
Port number . . . . . *ANY_____ 1-65535, *ANY

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

```

Figure 342. Trace TCP/IP Application (TRCTCPAPP) - SMTPSVR

Each of the parameters has a specific meaning, which are listed in Table 33.

Table 33. Parameters for TRCTCPAPP APP(*SMTPSVR)

Parameter	Option	Description
TCP/IP application	*SMTPSVR	Used for inbound mail.
	*SMTPCLT	Used for outbound mail.
Trace option setting	*ON	The collection of trace information is started.
	*OFF	The collection of trace information is stopped. The trace information is written to the spooled printer file.
	*END	Tracing is ended, and all trace information is purged. No trace information output is created.
	*CHK	The status of tracing for the specified application is checked. Messages are returned indicating whether tracing is active for the specified TCP/IP application the command parameters specified format the last time that TRCTCPAPP was started for this application, and other information related to the collection of trace information.
Maximum storage for trace	*APP	For *SMTPSVR or *SMTPCLT - 4096K per job.
	maximum KB	Specify the maximum amount of storage, in KB used to store trace records (one K equals 1024 bytes).

Parameter	Option	Description
Trace full action	*WRAP	When the trace buffer is full, the trace wraps to the beginning. The oldest trace records are written over by new ones as they are collected.
	*STOPTRC	Tracing stops when the trace buffer is full of trace records.
User Profile		The parameter is not used with *SMTPSVR or *SMTPCLT.
Recipient mail address	recipient-mail-address	Only trace information associated with a specific recipient mail address will be collected. This parameter is only valid when APP(*SMTPSVR) or APP(*SMTPCLT) is specified. Note: The recipient mail address (up to 255 characters) must have the following format: userid@abc.def.com
Remote Network Address		
Address Family	*INET	The the filter for AF_INET address family.
IP Address		The remote TCP/IP address for which trace information is to be collected.
Subnet mask		The subnet mask for which trace information is to be collected.
Port Number	*ANY	The TCP/IP port number defaults to *ANY, which implies traffic associated with any port on the remote system (and qualified by the IP address and subnet mask) will be traced. Note: If the user wants to specify the port, the subnet mask must also be specified.

7.7.3 SMTP outbound connections *SMTPCLT

Start TRCTCPAPP from the command line of the AS/400 system. Press **F4**. The screen shown in Figure 343 on page 258 appears. For the available parameters, see Table 34 on page 258.

```

Trace TCP/IP Application (TRCTCPAPP)

Type choices, press Enter.

TCP/IP application . . . . . > *SMTPCLT      *FTP, *SMTPSVR, *SMTPCLT...
Trace option setting . . . . . *ON           *ON, *OFF, *END, *CHK
Maximum storage for trace . . . *APP_____ 1-16000, *APP
Trace full action . . . . . *WRAP_____ *WRAP, *STOPTRC
Recipient mail address . . . . . _____
_____
_____

Recipient host name . . . . . _____
_____
_____

Domain name service . . . . . *NO_         *NO, *YES

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

```

Figure 343. Trace TCP/IP Application (TRCTCPAPP) - SMTPCLT

Table 34. Parameters for TRCTCPAPP APP(*SMTPCLT)

Parameter	Option	Description
TCP/IP application	*SMTPSVR	Used for inbound mail.
	*SMTPCLT	Used for outbound mail.
Trace option setting	*ON	The collection of trace information is started.
	*OFF	The collection of trace information is stopped. The trace information is written to the spooled printer file.
	*END	Tracing is ended and all trace information is purged. No trace information output is created.
	*CHK	The status of tracing for the specified application is checked. Messages are returned, indicating whether tracing is active for the specified TCP/IP application, the command parameters specified format the last time that TRCTCPAPP was started for this application, and other information related to the collection of trace information.
Maximum storage for trace	*APP	For *SMTPSVR or *SMTPCLT - 4096K per job.
	maximum KB	Specify the maximum amount of storage, in KB used to store trace records (one K equals 1024 bytes).

Parameter	Option	Description
Trace full action	*WRAP	When the trace buffer is full, the trace wraps to the beginning. The oldest trace records are written over by new ones as they are collected.
	*STOPTRC	Tracing stops when the trace buffer is full of trace records.
User Profile		The parameter is not used with *SMTPSVR or *SMTPCLT.
Recipient mail address	recipient-mail-address	Only trace information associated with a specific recipient mail address will be collected. This parameter is only valid when APP(*SMTPSVR) or APP(*SMTPCLT) is specified. Note: The recipient mail address (up to 255 characters) must have the following format: userid@abc.def.com
Recipient host name	recipient-host-name	Only trace information associated with a specific host name will be collected. The recipient host name (up to 255 characters) must have the following format: "abc.def.com" Note: This parameter is only valid when APP(*SMTPCLT) is specified.
Remote Network Address		
Address Family	*INET	The filter for AF_INET address family.
IP Address		The remote TCP/IP address for which trace information is to be collected.
Subnet mask		The subnet mask for which trace information is to be collected.
Port Number	*ANY	The TCP/IP port number defaults to *ANY which implies traffic associated with any port on the remote system (and qualified by the IP address and subnet mask) will be traced. Note: If the user wants to specify the port, the subnet mask must also be specified.
Domain Name Service	*NO	No filtering of trace information is done for DNS resolution.
	*YES	Trace information includes only trace points associated with DNS resolution and specifies whether only trace information associated with domain name service (DNS) resolution will be captured. This parameter is only valid when APP(*SMTPCLT) is specified.

7.8 AnyMail/MSF dump snap-in

This snap-in creates an AnyMail/MSF dump as a spooled file under user profile QMSF (WRKSPLF QMSF). One spooled file is generated each time MSF makes a pass through the piece of mail and calls the dump snap-in (for example, one spooled file for the MIME envelope and one spooled file for the attachment).

Follow these steps:

1. To activate the snap-in, type the following command on the OS/400 command line:

```
CALL QCMD
```

Press Enter.

Note: This starts the command line screen. To exit the command line screen, press the **F12** function key.

2. On the OS/400 command line, type:

```
ADDEXITPGM EXITPNT(QIBM_QZMFMSF_ACT) FORMAT(MSFF0100)
PGMNBR(200)PGM(QSYS/QZMFDUMP) TEXT('MSF Snap-in')PGMDTA(*JOB 12
SPCL01009999)
```

Press Enter. You need to use **F10** if you are prompting to see all the parameters.

Then, type:

```
ENDMSF
```

Press Enter.

On the OS/400 command line, type:

```
STRMSF *RESET
```

Press Enter.

3. Run the test scenario causing the issue.
4. Remove the MSF snap-in by typing the following command on the OS/400 command line:

```
ENDMSF
```

Press Enter.

Type the following command statement:

```
WRKREGINF QIBM_QZMFMSF*
```

Press Enter.

Select option **8** for **QIBM_QZMFMSF_ACT**.

Press Enter.

Remove the snap-in by selecting option **4** (=Remove) for Exit Program Number 200 which is **QZMFDUMP QSYS**.

Press Enter.

Type:

```
STRMSF *RESET
```

Press Enter.

5. To view the MSF Dump spooled files, use the following OS/400 command:

```
WRKSPLF SELECT(QMSF)
```

Press Enter.

Look for the spooled file **QPSRVDMP**.

7.9 Dumping Mail Server Framework (MSF)

This tool is for level 3 support only and is only mentioned here for completeness. The following process is performed.

1. Run the test scenario causing the issue.
2. Wait a sufficient amount of time for the test to complete.
3. On the OS/400 command line, type:

```
DMPYSOBY OBJ(QZMFMSF*) CONTEXT(QUSRSYS)
```

Press Enter.

Note: This command generates the QPSRVDMP spooled files.

4. To view the MSF dump, type the following command on the OS/400 command line:

```
WRKSPLF SELECT(QMSF)
```

Press Enter.

Look for spooled file **QPSRVDMP**.

7.10 Taking a communications trace of a line

This section describes the steps needed to collect trace data using the AS/400 system.

7.10.1 Collecting the line trace

To run a communications trace, perform the following steps:

1. On the OS/400 command line, type:

```
STRSST
```

Press Enter.

2. Select option **1** (Start a service tool), and press Enter.
3. Select option **3** (Work with communications trace), and press Enter.
4. Press **F6** (Start a trace). For the parameters, see Figure 344 on page 262.
5. Press Enter.

```

                                Start Trace

Type choices, press Enter.

Configuration object . . . . . tokenline

Type . . . . . 1          1=Line, 2=Network interface
                          3=Network server

Trace description . . . . . Comm Trace 1

Buffer size . . . . . 6          1=128K, 2=256K, 3=2M, 4=4M
                          5=6M, 6=8M, 7=16M, 8=32M
                          9=64M

Stop on buffer full . . . . . y          Y=Yes, N=No

Data direction . . . . . 3          1=Sent, 2=Received, 3=Both

Number of bytes to trace:
  Beginning bytes . . . . . *MAX      Value, *CALC, *MAX
  Ending bytes . . . . . *CALC      Value, *CALC

```

Figure 344. Starting the communications trace

6. On the next screen, for OS/400 V4R2M0 or above, select option **1** (all data (no filtering)), and press Enter.
7. To return to the OS/400 command line, press **F12** two times. Then, press Enter on the Exit System Service Tools screen.
8. Run the test scenario causing the issue.
9. To end the communications trace, complete the following tasks:
 - a. On an OS/400 command line, type:


```
STRSST
```

 Press Enter.
 - b. Select option **1** (Start a service tool), and press Enter.
 - c. Select option **3** (Work with communications trace), and press Enter.
 - d. On the Work with Communications Traces menu, select option **2** (Stop trace), and press Enter.
10. To format and print the collected data, select option **6** (Format and print trace), and press Enter.

Note: Ensure the parameters are set as shown in Figure 345 on page 263. If you know the IP addresses or port involved, you may want to specify these values to limit the amount of information placed in the printout.

```

                                Format Trace Data
Configuration object . . . . . : TRNLINE
Type . . . . . : LINE

Type choices, press Enter.

Controller . . . . . *ALL      *ALL, name

Data representation . . . . . 1      1=ASCII, 2=EBCDIC, 3=*CALC

Format RR, RNR commands . . . N      Y=Yes, N=No
Format Broadcast data . . . . N      Y=Yes, N=No
Format MAC or SMT data only . N      Y=Yes, N=No
Format UI data only . . . . . N      Y=Yes, N=No
Format SNA data only . . . . . N      Y=Yes, N=No
Format TCP/IP data only . . . . Y      Y=Yes, N=No
Format IPX data only . . . . . N      Y=Yes, N=No

F3=Exit      F5=Refresh      F12=Cancel

```

Figure 345. Format Trace Data

11. To view the file QPCSMPT, on the OS/400 command line, type:

```

WKRSPLEF
Press Enter.

```

7.11 Component Journaling

Component Journaling is available for V4R4M0, V4R3M0, and V4R2M0.

- V4R4M0
No PTF is required
- V4R3M0
PTF: SF55407, 5769TC1
APAR: SA78237
Note: SF55407 supersedes SF52765
- V4R2M0
PTF: SF55403, 5769TC1
APAR: SA78237
Note: SF55403 supersedes SF52765

To journal, complete the following process:

1. Start journaling in SMTP.

Prior to V4R4, you must create the data area QTMSJRNL in library QUSRSYS. To do so, on the OS/400 command line, type:

```

CRTDTAARA DTAARA(QUSRSYS/QTMSJRNL) TYPE(*CHAR) LEN(1) + VALUE('Y')
Press Enter.

```

Starting with V4R4, you need to change the SMPT attribute for journaling to *YES. To do so, on the OS/400 command line, type:

```
CHGSMTPA JOURNAL(*YES)
```

Press Enter.

2. Run the test scenario causing the issue.
3. Dump the journal receiver to file member JOURNAL1, in file JOURNAL, in library JRNLIB. On the OS/400 command line, type:

```
DSPJRN JRN(QZMF) OUTPUT(*OUTFILE) OUTFILE(JRNLIB/JOURNAL) +  
OUTMBR(JOURNAL1) ENTDTALEN(512)
```

Press Enter.

4. To display the file, use the following OS/400 command:

```
DSPPFM FILE(JRNLIB/JOURNAL) MBR(JOURNAL1)
```

Press Enter.

5. Stop journaling in SMTP.

Prior to V4R4, use the data area to control journaling. To disable journaling, while leaving the data area intact, on the OS/400 command line, type:

```
CHGDTAARA DTAARA(QUSRSYS/QTMSJRNL (1 1)) VALUE('N')
```

Press Enter.

Starting with V4R4, you need to change the SMTP attribute for journaling to *YES. To do so, on the OS/400 command line, type:

```
CHGSMTPA JOURNAL(*NO)
```

Press Enter.

Note: Specify VALUE('Y') to enable journaling. This can be done at any time and does not require restarting the SMTP, POP3, or MSF servers.

6. To delete the data area, type:

```
DLTDTAARA DTAARA(QUSRSYS/QTMSJRNL)
```

Press Enter.

7.11.1 AS/400 Mail Component Journaling Web page

For more information about component journaling, refer to the following Web site (this URL is case sensitive):

http://www.as400.ibm.com/tstudio/tech_ref/tcp/Indexfr.htm

7.11.2 Managing journal receivers

Journal records are stored in journal receivers. These receivers are user managed. When the journal becomes full, the user must issue the Change Journal (CHGJRN) command to change to a new journal receiver. The new SMTP Journaling function uses the QZMF journal.

7.11.3 Description of the major components

The major components involved in the delivery path are shown in Figure 346 on page 265.

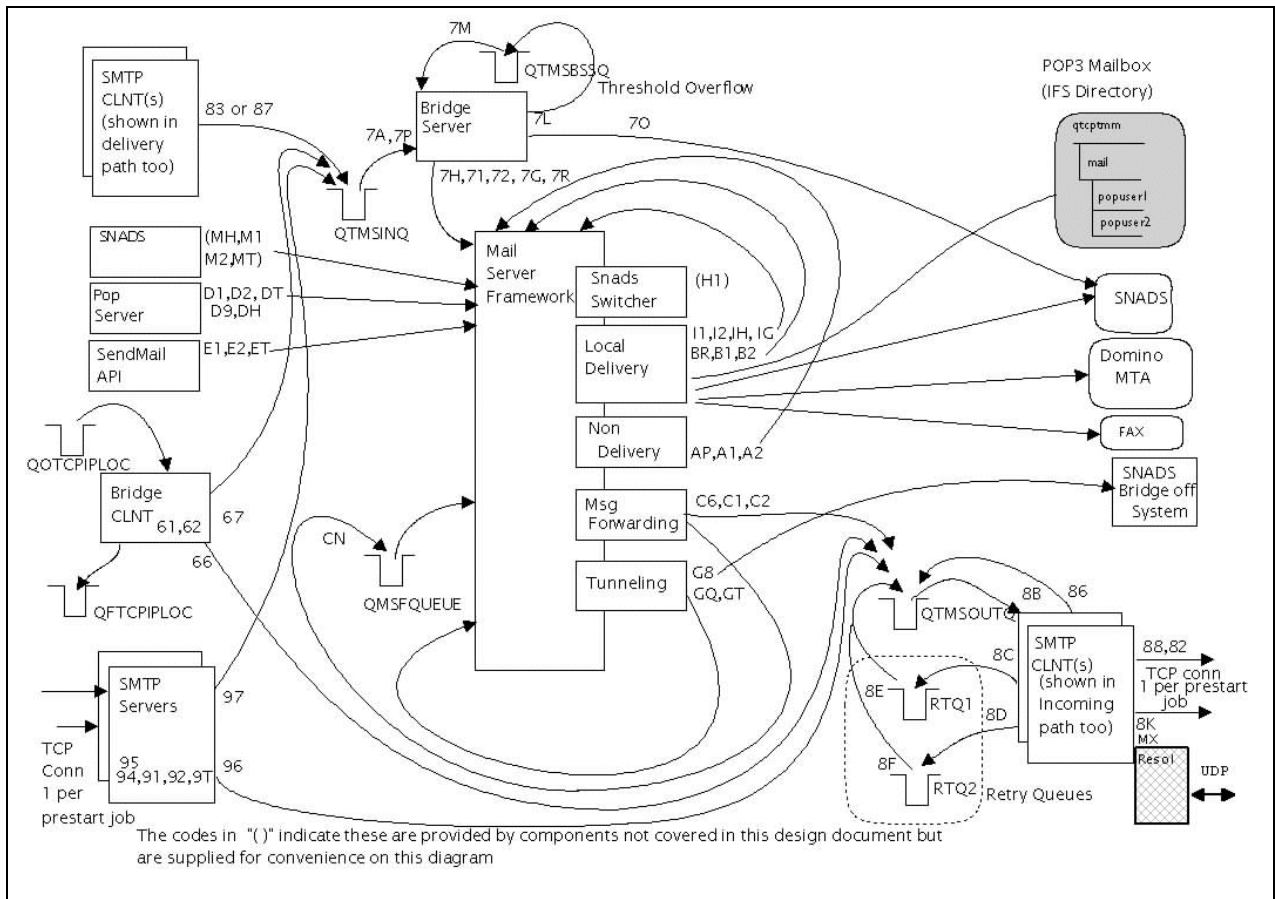


Figure 346. AS/400 Mail Components

Mail Server Framework

All incoming mail addressed to local recipients is channelled through this framework. Optionally, all the mail can be channelled through the framework in V4R4 if the parameter ALLMAILMSF is set to *YES using the (CHGSMTPA) command. The framework calls various exit programs, which are registered by address type. Different "snap-ins" (exit programs) are called, based on the recipient's address type.

QMSFQUEUE

Messages are stored in this queue when there is an abnormal return code passed back to MSF from one of the exit programs. This ensures that the mail will be retried when MSF is restarted (that is STRMSF with either the *RESUME or *RESET option; the *CLEAR option removes all the queue entries). The default value on the STRMSF command is *RESUME. We recommend the value *RESET. The value *RESUME picks up exactly where the error occurred, while *RESET brings the error to the top of the framework and restarts it.

The message ID in the QMSF job that indicates the job ended can be matched to the message ID in the journal, the MSFDUMP, or the SMTP trace. The message that indicates why the message was put in the MSF message queue is before the standard ending message that is put in the queue.

One of the most common reasons for errors is that the storage threshold is exceeded. This can be checked on the DSPSYSSTS screen. The typical threshold is 90%. One other common error that prevents message forwarding occurs when SMTP is started after MSF. MSF message forwarding ends if SMTP is not running. The recommended start order is SMTP followed by MSF.

SMTP Server

These programs (daemon plus prestart jobs for V4R4) implement the server portion of the SMTP protocol. They accept a message sent to the AS/400 host and either deliver the message into the MSF or relay the mail via the SMTP client. If the mail is for the MSF, it is placed into the incoming mail queue (QTMSINQ). If the mail is to be relayed, it is placed into the outgoing mail queue (QTMSOUTQ).

Bridge Clnt

This program removes the mail from the QOTCPIPLOC queue. SNADS writes outgoing messages to this queue. The program then puts the message in the standard SMTP message container and places the message on either the QTMSINQ or QTMSOUTQ queue.

SMTP Clnt

These programs (daemon plus prestart jobs for V4R4) implement the client portion of the SMTP protocol. They have the responsibility of resolving the recipient's hosts and then delivering the message for all the recipients on that host to the resolved address. The SMTP Clnt is driven by the arrival of the Mail message container.

MXResol

This is a routine called to resolve the host domain portion of a recipient's address. If the recipient has a host/domain that doesn't match the local AS/400 host/domain or any of its aliases, the MXResol is called.

QTMSINQ

This input queue drives the bridge server.

QTMSOUTQ

This queue drives the SMTP client. Message containers are placed on the queue when the messages are to be sent to remote systems.

Bridge Server

This program is responsible for removing the mail containers from QTMSINQ. All incoming mail is then dumped into the MSF, unless it was an undeliverable message or COD message that originated from the Bridge Client.

7.11.4 Journaling considerations

Journaling takes CPU cycles. Therefore, the best performance is realized when journaling is turned off. Journaling also takes up space on your AS/400 hard drives. However, if a mail problem occurs, journaling can offer insight into what happened to a particular piece of mail. To turn journaling on, a data area must be created. This data area, QTMSJRNL, resides in the QUSRSYS library.

Turning journaling on and off can be done at any time and does not require restarting the SMTP, POP3, or MSF servers. Note that the QMSFQUEUE to MSF transition only occurs when MSF is shut down and then restarted.

7.11.5 Viewing the journal receiver

As described earlier, the Journal entry output can be viewed by the DSPJRN command using "QZMF" as the JRN parameter. However, this gives a view of the LG records, which you must then display for the specific data stored along with the journal. It's probably easier to dump the journals into a file and then view the data via the DSPPFM command.

The following command dumps the journal receiver to a file member:

```
DSPJRN JRN(QZMF) OUTPUT(*OUTFILE) OUTFILE(JRNLIB/ZMFSTUFF) OUTMBR(MAR2)
ENDTALEN(512)
```

Here, JRNLIB is the name of the library, and ZMFSTUFF is the name of a physical file. The following command displays the file:

```
DSPPFM FILE(JRNLIB/ZMFSTUFF) MBR(MAR2)
```

Use **F20** to scroll to the right to see the journal-specific information.

Each journal entry has a two character SubType/Code preceding it, followed by any abbreviations and the information.

```
/* Some examples: */
/* 1. 94 LIN to SRVR 192.168.69.137 */
/* SMTP Server received local delivery message */
/* from host 192.68.69.137 */
/* 2. 91 O user1@server1.company.com */
/* Originator of Local message that precedes this */
```

The first character of the SubType/code consists of the function identifier for the entry. The function identifiers are listed in Table 35.

Table 35. Function identifiers

Function identifier	Description
1	MSF message created log entry
2	MSF message ended abnormally
3	MSF message reset by STRMSF command (STRMSF MSGOPT(*RESET))
4	MSF message removed by STRMSF command (STRMSF MSGOPT(*CLEAR))
5	MSF message acted on by address switcher
6	(not use4d in PTF versions) Bridge Client Entry
7	Bridge Server Entry
8	SMTP Client
9	SMTP Server
A	MSF Non Delivery
B	MSF Local Delivery
C	MSF Message Forwarding
D	POP Create Message

Function identifier	Description
E	Send Mail API
F	Domino MTA
G	Tunneling Snap-in
H	SNADS (Switcher)
I	MIME Parser (a local delivery snap-in)
L	FAX (Local Delivery)
M	SNADS

The second character of the SubType/code consists of the action that this journal entry is documenting. Table 36 identifies the second character of the code and documents the action taking place at the time of the journal. Table 37 on page 269 identifies the assorted journal entry abbreviations.

Table 36. Second character of SubType/code

JRN_CODE	Description
1	STC O Originator name follows
2	STC R Recipient name
3	STC U Undeliverable recipient
4	STC LIN TO SRVR IPADDR (from host)
5	STC RIN TO SRVR IPADDR
6	STC PGMNAME TO QTMSOUTQ
7	STC PGMNAME TO QTMSINQ
8	STC DLVED IPADDRESS (of host)
9	STC MSGID: <internal 822 Msg Id>
A	STC QTMSINQ TO PGMNAME
B	STC QTMSOUTQ TO PGMNAME
C	STC PGMNAME TO QTMSRTQ1
D	STC PGMNAME TO QTMSRTQ2
E	STC QTMSRTQ1 TO QTMSOUTQ
F	STC QTMSRTQ2 TO QTMSOUTQ
G	STC MSGID MAP TO < MSF ID >
H	STC PGMNAME to MSF
K	STC RESERR errno domain
L	STC PGMNAME TO QTMSBSSQ
M	STC QTMMBSSQ TO PGMNAME
N	STC PGMNAME TO QMSFQUEUE
O	STC PGMNAME to SNADS

JRN_CODE	Description
P	STC UNDELIVERABLE NOTICE
Q	STC LOCAL DEL BY TUNNELING
R	STC CRT COD MSG
S	STC SPAM CONN DENIED IPADDR
T	STC MSG SIZE

Table 37. Journal entry abbreviations

Abbreviations	Description
LIN	Local in, received a note for local delivery, IP address that follows is host that sent the note
RIN	Relay in, received a note to relay to another SMTP daemon. IP addr that sent it follows
R	Recipient
O	Originator
U	Undeliverable Recipient
QTMSINQ	Input queue of SMTP
QTMSOUTQ	Output queue of SMTP
QTMSBSSQ	Holding queue where messages are place when System Storage Threshold is exceeded.
QTMSRTQ1	First level retry queue
QTMSRTQ2	Secondary level retry queue
RRSL	Recipient Resolved

7.11.6 Mail Server journal entries

Mail Server journal entries are currently made for SMTP, MSF, and SNADS switching. They are shown in Table 38 through Table 44 on the following pages.

Note: All of the journal entries documented here use the LG type, which stands for "log entry."

Table 38. Mail Server journal entries

Type	Action	SubType/Code(s)	Comments
LG	Checking availability	CN	Record MsgId that was put back on QMSF queue due to SMTP not being started.
LG	Enqueuing the mail	C6 C1 C2	Log mail being put onto QTMSOUTQ

Table 39. SMTP client

Type	Action	SubType/Codes	Comments
LG	Dequeuing of container for processing	8B	Just after floater tag is set log dequeue of Mail
LG	successful mail delivery	88	Log each successfully send to recipient
		82	Plan to log each recipient too.
LG	Undeliverable mail	83	Log undelivered mail
LG	1st level timeout	8C	Log when adding to 1st level retry queue
LG	2nd level timeout	8D	Log when adding to 2nd level retry queue
LG	mail is ready to be retried	8E	Log when retried mail put back on QTMSOUTQ
		8F	
LG	COD being sent back to originator	87	Log when COD is enqueued on BRSR queue
LG	Cannot process, resource busy	86	Log when mail gets put back on QTMSOUTQ because connection matrix full
LG	examine recipient records	86	Log when mail gets put back on QTMSOUTQ because recipient status changed, ie MX record resolved ready to deliver the message.
LG	undeliverable	87	Log transfer of mail to QTMSINQ for undeliverable notice, two places
LG	MX query	8K	Log a res_send failure and errno of why it failed along with query buffer

Table 40. SMTP Serve

Type	Action	SubType/Codes	Comments
LG	receiving mail	94	Log reception of mail just after receiving ending sequence CRLF <.>CRLF (local) Originator and recipient are logged. Message Size nnnnn where nnnnn is the number of bytes. MsgId
		91	
		92	
		9T	
		99	
LG	receiving relayed mail	95	Log MAIL just after receiving ending sequence CRLF <.>CRLF (relayed) Originator and recipient are logged
		91	
		92	
LG	passing off mail to Bridge client	97	Log entry of MAIL into QTMSINQ (incoming mail)
LG	passing off mail to client for remote delivery	96	Log entry of MAIL into QTMSOUTQ (relayed mail)

Table 41. Bridge server

Type	Action	SubType/Codes	Comments
LG	Getting mail off of the "IN" queue	7A	Log mail being dequeued from QTMSINQ
LG	passing off mail to SNADS	7O	Record successful transfer to QSNADS
LG	putting container on the "BUSY" queue because of space usage.	7L	Record when mail is enqueued on QTMSBSSQ because of threshold overflow
LG	getting mail off of "BUSY" queue	7M	Record dequeuing mail from QTMSBSSQ, space was reclaimed and the mail can now be processed.
LG	pass message to MSF	7H 71 72	Record when message gets inserted into framework
LG	creation of COD message	7R 7G	Record when COD message gets inserted into framework Log the MSF MSGID since the new COD message is being created.
LG	cannot deliver this piece of mail to a recipient	7P 7G	Log the fact that we're creating an undeliverable notice Log the MSGID of the new undeliverable msg notice.

Table 42. Additional MSF and POP journal points

Type	Action	SubType/Codes	Comments
LG	reinsertion of parsed MIME note into framework	IH	Log when the parsed MIME message is reinserted into the MSF.
		I1	
		I2	
		IG	
LG	sending COD message into MSF	BR	Record insertion of COD message into the MSF
		B1	
		B2	
LG	creation of nondelivery message	AP	Record non Delivery message being inserted into MSF
		A1	
		A2	
LG	POP receives message from MAPI client and sends it into MSF	D1	Record POP inserting message into the MSF (This is a use of the XTND XDESCRIPT) Size of Message Log RFC822 MSGID POP3 to MSF xfer
		D2	
		DT	
		D9	
		DH	

Table 43. Additional MSF and POP journal points

LG	use of the Sendmail API	EH	Record creation of message by SendMail API Message Size nnnnn where nnnnn is size of message (all attachments)
		E1	
		E2	
		ET	
LG	Mail is targeted to a SNADS bridged remote system	G8	Record when message is tunneled. Include system sent to.
		G2	Recipient
LG	Mail tunneled through a SNADS bridge is received.	GQ	Record receiving tunneled message for local delivery
		G2	Recipient
LG	Mail is delivered into a POP mail box	B8	Record delivery of message to local pop mail box, ipaddress will be pop mailbox directory. Recipient will also be listed.
		B2	

Table 44. Journaling points not in SMTP or the framework

Type	Function	SubType/Code(s)	Comments
LG	Address resolution SNADS switches either from/to	H1	SNADS switched a message into the MSF

7.12 EDTF

Note that EDTF is a program used to read files in the root file system of the integrated file system (IFS) on the AS/400 system. Depending on the OS/400 Version of your AS/400 system, you need to load one of the following PTFs. The EDTF command is included in OS/400 V4R4.

- For **V4R3M0**, use PTF: SF49052 (APAR SA69146, 5769SS1)
- For **V4R2M0**, use PTF: SF45296 (APAR SA69146, 5769SS1)
- For **V4R1M0**, use PTF: SF41518 (APAR SA65156, 5769SS1)
- For **V3R7M0**, use PTF: SF38832 (APAR SA61798, 5716SS1)

7.13 Web site for PTF cover letters and APARS

The following Web site contains PTF cover letter information:

<http://as400service.ibm.com/>

Select **Tech Info & Databases**, and select **PTF Cover Letters**

7.14 POP3 Mail

This section provides information about POP3 mail problem determination.

7.14.1 Tips on debugging mail on an AS/400 system

When mail is not being delivered as expected, a DNS/Mail administrator is faced with one of the most challenging troubleshooting areas in TCP/IP.

7.14.1.1 The starting and ending place

The first step in debugging mail is to always know exactly what the users are using to address the mail. If possible, visit the users at the client location and watch them type in the "Mail To" value: <user Id@smtp domain name>. Watch for mis-typing. Make sure that the user is using the @ symbol and not using the word *at*.

The second step is to find the SMTP User ID and the SMTP Domain name in the AS/400 system alias table on the AS/400 system for the POP client to which the mail should be delivered.

These two pieces of information are the starting and ending place for mail. Mail delivery starts by using the "Mail To:" information and ends by delivering the mail to the POP mailbox on the AS/400 system associated with the SMTP User ID and the SMTP Domain name.

What the user types to the right of the @ sign in the "Mail To" field should match the SMTP Domain name in the AS/400 SMTP system alias table for the POP3

user who should be receiving the mail with *one exception*: when aliases are used. For example, consider when mail is addressed to:

user@mycompany.com

However, the AS/400 SMTP system alias table lists this user's SMTP Domain name as *AS1.mycompany.com*. This discrepancy is okay and mail is successfully delivered if AS1's local host table lists *mycompany.com* as an alias to *AS1.mycompany.com* and the Search First parameter in CFGTCP option 12 is set to *LOCAL.

7.14.1.2 The POP3 directory entry

The POP3 directory entry can be a source of confusion for an AS/400 administrator configuring POP3 for the first time. What makes a directory entry a POP3 directory entry?

The answer is: two parameters in the directory entry determine if the entry is a POP3 directory entry. The parameters are:

- Mail Service Level = 2 (System message store)
- Preferred address = 3 (SMTP name)

Tip

The POP directory entry needs to be configured on the AS/400 system that is the final resting place for the mail (until the user "Gets the Mail"). This is the AS/400 system of which the POP3 client continues its Incoming POP Server. It is the AS/400 system where the POP3 client "gets" mail. There is another kind of directory entry that can be used to forward mail. It is a different type of directory entry from the POP directory entry.

TCP/IP configuration

Verify that the SMTP client sending the mail and the POP client receiving the mail have TCP/IP connectivity to their respective servers. Also, verify that each client can successfully ping their server by IP address. If the ping is not successful, you need to debug a TCP/IP connectivity problem before proceeding to debug a mail problem:

- Make sure the appropriate AS/400 line descriptions are active.
- Verify that the associated IP interface has been started on the AS/400 system.
- Verify that the TCP/IP route exists if the client is on another subnet from the SMTP, POP, or DNS server.

If the mail client is configured to have the SMTP Outgoing Mail Server or Incoming Mail Server to be a host.domain name rather than an IP address, verify that a ping to the host name is successful. If a ping by IP address works but a ping by host name fails, you need to debug a DNS problem before proceeding to debug a mail problem.

7.14.1.3 DNS server

Verify the DNS server is started and an active QTOBDNS job exists in QSYSWRK subsystem. Check its job log for errors. Verify that the IP interfaces to which the DNS server should be bound are started, including the Internet address listed on the same AS/400 system's CFGTCP option 12.

If changes or corrections have been made to the DNS server, make sure the DNS server has been updated to pick up those changes.

Use NSLOOKUP to verify that the DNS server is responding with the answers you expect. For example, is the DNS server resolving the SMTP domain name used to the right of the @ symbol in the "Mail To" address? If not, this can be a problem, unless an alias is used in the AS/400 local host table and Searched First =*LOCAL is used.

7.14.1.4 SMTP and POP servers

Verify that the SMTP and POP servers are active. If they are active, their corresponding jobs are listed as active jobs in the QSYSWRK subsystem. Enter the following command:

```
WRKACTJOB SBS (QSYSWRK)
```

Then, page down.

If the SMTP server is active, you should find four SMTP jobs named as shown here:

```
QTSMPBRCL  
QTSMPBRSR  
QTSMPCLNT  
QTSMPSRVR
```

If the POP server is active, locate one or more jobs with the following three names:

```
QTPOP00622  
QTPOP00635  
QTPOP00681
```

The last five numbers in the POP job name can be any number. Also, even one QTPOPxxxxx job active indicates that the POP server is active. If the preceding jobs do not exist under QSYSWRK subsystem, then start the missing servers.

To start the SMTP server, use:

```
STRTCPSVR SERVER (*SMTP)
```

To start the POP server, use:

```
STRTCPSVR SERVER (*POP)
```

If you use either or both of these commands and still cannot find the associated active jobs in the QYSWRK subsystem, it is possible that these jobs are starting but ending before you can locate them. First, check for any errors in the user job log that issued the STRTCPSVR commands. If your own interactive job was used to issue the commands, review your own job log with the following command:

```
DSPJOBLOG
```

Press Enter, followed by **F10**. Then, page up to look for error messages.

Also, if the SMTP or POP jobs are ending with an error, review their spooled job logs for error messages. These jobs run using the QTCP user profile. Therefore, to find the spooled job logs of the inactive jobs, use the following command:

```
WRKSPLF QTCP
```

Press Enter, followed by **F18**, to go to the bottom of the list. The job name is usually displayed in the User Data field in the Work With Spooled Files display.

If the SMTP and POP jobs are active and mail is still not being delivered, always check the SMTP and POP active job logs for any error messages. Any error messages in these job logs can give you clues as to what is going wrong.

Tip

If changes to the AS/400 TCP/IP domain or host table were made with the CFGTCP command, option 12 or option 10, the SMTP server needs to be ended and started again to pick up the changes.

7.14.1.5 QMSF job

For mail to be successfully delivered on an AS/400 system, at least one QMSF job needs to be active under the QSYSWRK subsystem. This job should autostart when the QSYSWRK subsystem goes active. However, certain errors can cause the QMSF job to end. Therefore, if mail is not being delivered, verify that QMSF is active. To do so, issue the following command:

```
WRKACTJOB SBS(QSYSWRK)
```

QMSF should be listed as an active job. If it is not listed, you can start the QMSF job by issuing the following command:

```
STRMSF
```

If you issue the Start Mail Server Framework (*STRMSF*) command and still cannot find QMSF as an active job under QSYSWRK, the job may be starting but ending right away with an error. If this is the case, the ended job log should be reviewed for error messages. The QMSF job runs using the QMSF user profile. To find the spooled file for the QMSF job log, issue the following command:

```
WRKSPLF QMSF
```

Press **F18** to go to the bottom of the list. Many of these QMSF job log spooled files may be listed. Use the **F11** key to display the date and time stamps of these jobs to help locate the one that you need.

If the QMSF job is active and mail is still not being delivered, check the active QMSF job log for errors.

7.14.1.6 IBM Firewall for the AS/400 system

If the IBM Firewall is involved in the network configuration and the mail should be flowing across the firewall, verify that the firewall is active with the following command:

```
WRKCFGSTS *NWS <firewall name>
```

If it is not active, you may vary it on with option 1 from the *WRKCFGSTS* display.

Verify that the secure mail server is configured correctly on the firewall. You may have made changes to the AS/400 TCP/IP domain information using CFGTCP option 12. Therefore, the firewall's network server description is configured to use this information. If this is the case, you must vary off and vary back on the firewall network server description to pick up the changes.

If mail inbound from the Internet is not reaching the secure mail server, you can check the mail queue on the firewall. If the mail makes it to the firewall, but the firewall cannot relay it, the mail is left on the firewall in the mail queue.

To check the mail queue, use the Submit Network Server Command (`SBMNWSCMD`) command on an AS/400 command line to make a directory of the directory. Issue a command on the firewall with the `DIR` command for the directory:

```
K:\firewall\mqueue\
```

If the mail is still on the firewall's mail queue, its control file may contain useful information. The control file begins with a "q" (for example, qfRAA002.11). The associated data file begins with a "d" (such as, dfRAA002.11).

You may want to check the mail log located in: `E:\mptn\etc\mail.log`

You also may want to check the error file, which is a file that only exists if there is a mail problem. The error file is located in: `E:\mptn\etc\sendmail.err`

For additional information on firewall problem determination including mail, refer to *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162.

7.14.1.7 The POP mailbox on the AS/400 system

When POP3 mail is successfully delivered on the AS/400 system, it is located in a "POP mailbox" on the AS/400 system until the POP3 user issues the GET MAIL command from the POP3 client. It is possible to review the contents of an AS/400 IFS directory to determine if a POP3 user has any mail distributions in the POP3 mailbox. This is useful when debugging a mail problem because an administrator does not have to continue to use the POP3 client and issue the GET MAIL command to see if mail is finally working. Instead, they can check for mail with one green-screen command, which is:

```
WRKLNK ' /QTCPTMM/MAIL/JONEST2 '
```

Here, JONEST2 in the command is the system directory user ID of the POP3 client. This may be different from their SMTP user ID.

If the POP3 mailbox exists, the previous command produces the display shown in Figure 347 on page 279.

```

Work with Object Links

Directory . . . . : /QTCPTMM/MAIL

Type options, press Enter.
 3=Copy  4=Remove  5=Next level  7=Rename  8=Display attributes
11=Change current directory ...

Opt  Object link      Type  Attribute  Text
    JONEST2           DIR

Parameters or command
Bottom

```

Figure 347. Locating a POP3 mailbox on the AS/400 system

Note

If the previous command is issued and the error message `Object not found` is issued to the user's job log, the POP3 mailbox does not exist. It is important to realize that the POP3 mailbox does not exist until the first distribution of mail is delivered to it. If the POP3 mailbox (in the form of the directory listed in Figure 347) is missing, it does not necessarily mean that the POP3 directory entry was misconfigured. It may just mean that mail has never been delivered to this mailbox.

From the display in Figure 347, select option **5** to view the next level. The next level shows any mail distributions that exist in the POP3 mailbox. The screen displayed in Figure 348 on page 280 shows that the two mail distributions are located in the JONEST2 POP3 mailbox. These distributions disappear after the POP3 user issues the GET MAIL command from the POP3 client. You cannot read the contents of these mail distributions from an AS/400 green screen.

```

Work with Object Links

Directory . . . . : /QTCPTMM/MAIL/JONEST2

Type options, press Enter.
3=Copy 4=Remove 5=Next level 7=Rename 8=Display attributes
11=Change current directory ...

Opt  Object link      Type  Attribute  Text
     JW122040.NOT     STMF
     JW122735.NOT     STMF

```

Bottom

Figure 348. Mail distributions in the JONEST2 POP3 mailbox on the AS/400 system

7.15 Tools for e-mail monitoring with Domino

Domino provides three tools that you can use to monitor mail. Message tracking allows you to track specific mail messages to determine if the intended recipients received them. Mail usage reports provide the information you need to resolve mail problems and improve the efficiency of your mail network. Mail probes test and gather statistics on mail routes.

7.15.1 Tracking mail messages

Both Domino administrators and end users can track mail. Administrators can track mail sent by any user, while end users can track only messages that they themselves send.

When you configure mail tracking, you can specify which types of information Domino records. For example, you can specify that Domino won't record message tracking information for certain users, or you can choose not to record the subject line of messages sent by specific users.

Domino records all message tracking information in the Mail Tracking Store database (MTSTORE.NSF). When an administrator or user searches for a particular message, Domino searches the Mail Tracking Store database, which is created automatically when you start the Mail Tracking program on the server.

7.15.2 How mail tracking works

Mail tracking follows this process:

1. Create a query to determine whether a specific message arrived at its intended destination or to determine how far it got if delivery failed.
2. Message tracking begins on the starting server. If the message is found there, the tracking automatically continues on the next server on the route.
3. Step 2 is repeated on each "next server" until the route ends. Detailed information is provided about the processing of the message on each server.

4. Select the message, and then check the delivery status. The types of status are shown in Table 45.

Table 45. Domino Message Tracking - Delivery status

Delivery Status	Meaning
Delivered	The message was delivered to a mailbox on the server. The mailbox status indicates whether the message was read, unread, or deleted. If the mailbox status is not read, unread, or deleted, it appears as unknown.
Delivery failed	The server attempted to save the message in a mailbox but was unsuccessful. The addressee may not exist or the server's disk may be full.
In queue	The router is processing the message.
Transferred	The router successfully sent the message to the server identified in the next hop field.
Transfer failed	The router attempted to transfer the message to another server and failed.
Group expanded	The message was addressed to a group and the group was expanded on this server.
Unknown	That status of the message on the server cannot be determined.

7.15.3 Generating mail usage reports

Over time, the Mail Tracking Store database stockpiles historical data about messaging on the server. It may be useful to generate mail usage reports from this data. For example, you can generate reports of recent messaging activity, message volume, individual usage levels, and heavily travelled message routes.

Mail usage reports provide important information that you can use to resolve problems and improve the efficiency of the mail network. In addition, this information is valuable when you plan changes or expansions to the mail network. For example, you can generate a report that shows the top 25 largest messages or the top users by the number and size of messages. With this information, you can identify users who may be misusing your mail system. Reports showing the most popular next and previous hops can help you assess compliance with corporate mail use policies.

Domino uses the data stored in the Mail Tracking Store database (MTSTORE.NSF) to create mail usage reports. As an administrator, you can generate a one-time report, or you can generate scheduled reports. By default, Domino generates scheduled reports at midnight at the interval you specify, for example daily, weekly, or monthly.

The Reports database (REPORTS.NSF) stores all mail usage reports. Views in the database display reports according to report type, date, and user. In addition, a view displays all scheduled reports by interval.

7.15.4 Mail probes

You can monitor your mail network by configuring probes to test and gather statistics on mail routes.

7.15.4.1 Creating a mail probe

Using a mail probe, you can test and gather statistics on mail routes. To test a mail route, use the ISpy task. ISpy sends a mail-trace message to the mail server of the individual that you specify. The probe generates a statistic that indicates

the amount of time, in seconds, that it took to deliver the message. If the probe fails, the statistic has the value -1. The format of a mail probe statistic is:

QOS.Mail.RecipientName.ResponseTime

If the Collect task is running, the Statistics database (STATREP.NSF) stores the mail probe statistics. In addition, ISpy generates events for probes that fail. You can set up an Event Notification document to notify you when an event has occurred. By default, ISpy monitors the local mail server. To monitor other Domino mail servers, you must create probe documents.

7.15.4.2 Creating a mail probe

Complete these steps to create a mail probe:

1. Make sure that you start the **ISpy task** on the server.
2. From the Domino Administrator, click the **Configuration** tab.
3. Click **Statistics & Events->Probes->Mail**.
4. Click **New Mail Probe**.
5. Click the **Basics** tab, and complete the following fields shown in Table 46.

Note: Do not select *All Domino servers in the domain will probe themselves*.

Table 46. Fields to complete on the Basics tab for a mail probe

Field	Enter
Probing servers (source)	Enter the server you want the probe to start from or select the server from the drop-down box.
Target mail address (destination)	Enter the mail recipient for which you want to check the mail route or use the drop-down box to select a recipient from a Domino Directory or Address Book. Do not enter more than one individual and do not enter a group name.

6. Click the **Probe** tab, and complete the fields shown in Table 47.

Table 47. Fields to complete on the Probe tab for a mail probe

Field	Enter
Send interval:	Enter the probe interval. This is the frequency at which probes will be sent.
Time out threshold	Enter the time out threshold. This is the period the probing server (source) will wait for a response before logging a failure.

7. Click the **Other** tab. Complete the fields as shown in Table 48, and then click **OK**.

Table 48. Fields to complete on the Other tab for a mail probe

Field	Enter
Event	Select the severity of the event you want to be generated if the probe fails.
Create a new notification profile for this event.	You can set up notification for a custom event. If you click this button, you will be guided through the process by the Event Notification Wizard.
Enablement	Select the "Disable the probe" field if you want to disable this probe. You can re-enable it at any time.

7.16 Setting up the Reports database for Domino

The Reports database (REPORTS.NSF) must be loaded on the server in order to generate mail usage reports. Typically, the Reports database is created automatically when you set up the server.

If you need to create the Reports database, choose **File->Database->New**.

Complete the fields as shown in Table 49.

Table 49. Values for creating the Reports database

Field	Enter
Server	The name of the server that stores the Mail Tracking Store database (MTSTORE.NSF)
Title	Reports
File name	Reports.nsf
Template	Reports.ntf

7.16.1 Security

The Reports database is automatically created when the server is set up. However, for security purposes, you must perform the following steps manually:

1. View the Access Control List (ACL), and verify that the administrator of the server and the server itself are present and have manager access.
2. Select the **View->Agents** list box and enable all scheduled agents.
3. Give the administrator unrestricted agent access on the server by adding them to the server document. Select **Security->Agent Restrictions->Run unrestricted LotusScript/Java agents**.

7.17 Controlling the Mail Tracking Collector

Before you can use mail tracking data for tracking or reports, it must be collected in the Mail Tracking Store database (MTSTORE.NSF).

Table 50 on page 284 shows the functions available in the main tracking collector and the Domino console commands used to implement the function.

Table 50. Tasks for managing mail tracking

To do this	Perform this task
Automatically start mail tracking on a server when the server starts	Tracking starts when the Router starts.
Automatically stop Mail Tracking Collector on a server when the server stops	Tracking stops when the Router stops.
Manually start mail tracking	Enter the command load mtc at the console.
Manually stop mail tracking	Enter the command tell mtc quit at the console.
Manually tell the Mail Tracking Collector to collect	Enter the command tell mtc process at the console.
Manually tell the Mail Tracking Collector to use a different collection interval	Enter the command tell mtc interval < value > at the console, where <i>value</i> is the number of minutes to use.
Manually tell the Mail Tracking Collector to compact the Mail Tracking Store database	Enter the command tell mtc compact at the console.
Manually tell the Mail Tracking Collector to reindex the Mail Tracking Store database	Enter the command tell mtc reindex at the console.
Manually tell the Mail Tracking Collector to purge the Mail Tracking Store database	Enter the command tell mtc purge < value > at the console, where <i>value</i> is a number of days. All entries in the Mail Tracking Store database older than <i>value</i> will be purged.

7.18 Configuring the server for message tracking

This process allows you to customize the type of information you want to collect and store in the Mail Tracking Store database (MTSTORE.NSF). For example, you can exclude certain users' mail from being collected, or you can restrict messages from being tracked by message subject. Follow these steps:

1. From the Domino Administrator, click the **Configuration** tab.
2. Expand the **Server** view.
3. In the Use Directory on field, choose **Current Server**.
4. Perform either Step 5 or Step 6, depending on whether you need to create a new Configuration Settings document.
5. To create a new Configuration Settings document, follow these steps:
 - a. Click **Configurations**, and then click **Add Configuration**.
 - b. Click the **Basics** tab.
 - c. Click **Yes** in the Use these settings as the default settings for all servers check box to use this Configuration Settings document for applying to all servers. Otherwise, enter the name of a specific server or group in the Group or Server name field.
 - d. Leave all other fields as their default.
 - e. Click **Save and Close**.
6. Click **Configurations**, and then double-click the name of the server for which you want to enable message tracking.
7. In the Configuration Settings document, click the **Router/SMTP - Message Tracking** tab.

8. Click **Edit Server Configuration**.

9. Complete the fields shown in Table 51, and then click **Save and Close**.

Table 51. Server configuration fields for message tracking

Field	Enter
Message tracking	Choose one: <ul style="list-style-type: none"> • Enabled to log message-handling activity information in the Mail Tracking Store database • Disabled (default) to not log any message-handling information
Don't track messages for	The names of users and/or groups whose messages will not be logged and, therefore, cannot be tracked. This field applies only to messages sent by the specified person or group. For example, you may decide that you do not want administrators to be able to track the messages sent by the Manager of Human Resources at your organization. In this case, you enter the name of that user in this field. If you leave this field blank (default), authorized administrators can track messages for all users and groups on all servers that are enabled for mail tracking.
Log message subjects	Choose one: <ul style="list-style-type: none"> • Yes to log message subjects in the Mail Tracking Store database • No (the default) to not log message subjects
Don't log subjects for	The names of users and/or groups whose message subjects will not be logged and, therefore, cannot be tracked. This field applies only to messages sent by the specified person or group. The default is none.
Message tracking collection interval	A number that represents how often, in minutes, you want to log message tracking activity in the Mail Tracking Store database. Note This number may affect server performance. Enter a number appropriate to the size and speed of your system. The default 15 minutes is recommended.
Allowed to track messages	The names of servers and/or users allowed to track messages on this server. If you leave this field blank (default), only members of the LocalDomainServers group are authorized to track messages on this server. If you add any entries to this field, you must list <i>*/</i> servers and/or users that are allowed to track messages on this server.
Allowed to track subjects	The names of servers and/or users allowed to track messages by subject on this server. If you leave this field blank (default), only members of the LocalDomainServers group are authorized to track messages by subject on this server. If you add any entries to this field, you must list <i>*/</i> servers and/or users allowed to track subjects on this server. Note If you list servers and/or users in this field, you do not have list them in the "Allowed to track messages" field.

Keep in mind that the Mail Tracking Store database becomes larger as information is collected from the Router. If disk storage space is a concern, use database replication. The number of days restricts how far back in time that messages can be tracked. Therefore, choose a value that balances tracking needs and available disk storage.

7.19 Tracking a mail message

Figure 349 on page 286 shows the graphical user interface (GUI) of the Domino Message Tracking Tool. The following steps explain how to use Domino Message Tracking.

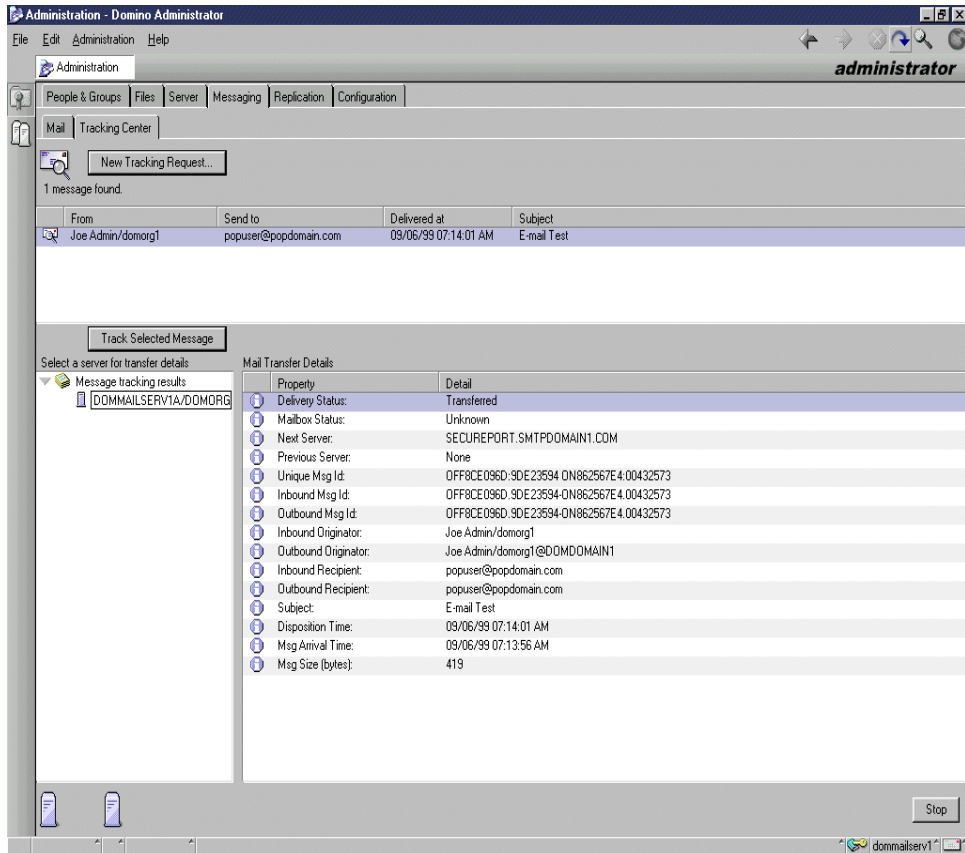


Figure 349. Graphical user interface for Domino Message Tracking

If you track a mail message and the search finds no messages, adjust the search criteria and then perform the search again. Follow this series of steps:

1. Make sure that you set up mail monitoring.
2. From the Domino Administrator, click the **Messaging - Tracking Center** tab.
3. Click **New Tracking Request**.
4. Complete any of the fields shown in Table 52 on page 287 to describe the message that you want to track. Then, click **OK**.

Table 52. Message tracking options

Field	Enter
From	The user name of the sender. Note You can also select the name from the Domino Directory.
To	The user name of the recipient. Note You can also select the name from the Domino Directory.
Sent	Choose one: <ul style="list-style-type: none"> • Today • Yesterday • Last week • Last 2 weeks • Last month • All times Note To increase the likelihood of finding messages, choose a long time period.
Start	Choose one: <ul style="list-style-type: none"> • Sender's home server (default) • Current server If you know the sender of the message, you can start the search at the sender's home server. If you don't know the sender of the message and you leave the From field blank, choose "Current server" as the search start. If you manage multiple servers, you can change the current server by selecting a server name from the bookmark pages at the left of the screen.
Subject	The subject of the message that you want to track. Note The server must be configured to allow tracking by subject.
Message ID	The message ID of the message you want to track. Note The message ID appears in the Mail Tracking Store database (MTSTORE.NSF).

5. In the Messages Found panel, select a message. Then, click **Track Selected Message**.
6. Expand **Message tracking** results, and select a server to see the detailed information about what happened to the message on that server (optional).

Chapter 8. Installing a Windows NT Server to support firewalls

This chapter summarizes information found in the redbook *AS/400 - Implementing Windows NT on the Integrated Netfinity Server*, SG24-2164. You should refer to that redbook for complete details about how to install Windows NT Server 4.0 on the Integrated Netfinity Server. This chapter contains the information we used to install and configure our firewall on an Integrated Netfinity Server.

8.1 Overview

Before you attempt to install Windows NT Server on the Integrated Netfinity Server, complete the following checklists:

- Hardware checklist
- Software checklist
- Installation worksheet

Both checklists are presented in 8.5, “Hardware and software checklists” on page 296. The installation worksheet is presented in 8.6, “Installation worksheets” on page 297.

The installation worksheet is important because you need this information to enter values in the Install Windows NT Server (INSWNTSVR) command. The descriptions in the worksheet explain each parameter to ensure that you have the correct information ready when you start the installation.

The Windows NT firewall should be configured as a dual-homed firewall. This requires two LAN adapters on the Integrated Netfinity Server, in addition to the *INTERNAL PORT. These LAN adapters should *not* have AS/400 TCP/IP interfaces defined for them. The AS/400 system should have a separate LAN adapter that is used by OS/400 TCP/IP to access the secure network.

If you do not have space for an additional LAN adapter, you may use indirect routing through the secure port of the firewall to access the AS/400 system using the virtual LAN adapter. This is not recommended because it increases the workload on the firewall.

If you have difficulty determining the correct values for the worksheets, refer to *AS/400 - Implementing Windows NT on the Integrated Netfinity Server*, SG24-2164.

8.2 AS/400 planning

Before installing Windows NT Server on the Integrated Netfinity Server, you need to plan for the AS/400-related items described in the following sections.

Disk storage requirements

Setting up a Windows NT server on the Integrated Netfinity server requires these amounts of disk storage:

- **OS/400 - AS/400 Integration for NT (5769-SS1 option 29)**

50 MB of disk storage is used when you load 5769-SS1 option 29 on your AS/400 system.

- **Windows NT Server**

You need an absolute minimum of 1 GB of free disk space available on your AS/400 system before setting up a Windows NT server on the Integrated Netfinity server. The 1 GB only applies if you choose to configure the minimum values for the Windows NT D: and E: drives. This size does not provide much additional space for other items such as log files. We recommend 2 GB for the E: drive. Refer to 8.4, "Disk storage sizing considerations" on page 294, for more information on estimating disk storage requirements for your server.

TCP/IP

The TCP/IP Utilities program product (5769-TC1), which is supplied free of charge, is *not* required to install Windows NT Server on an Integrated Netfinity Server. OS/400 (5769-SS1) contains all the necessary TCP/IP functions. However, you should still install TCP/IP Utilities to support functions such as Telnet, FTP, DNS, SMTP, and so on.

LAN adapters

For the firewall, you must have two LAN adapters that are under the exclusive control of the Integrated Netfinity Server to communicate with the secure and non-secure network. You must also have at least one additional LAN adapter for the use of OS/400 TCP/IP for communications with the secure network. The shared adapter configuration *is not supported*. This means that you must have a minimum of three LAN adapters installed on the AS/400 system. The LAN adapters used by the Integrated Netfinity Server *should not* be configured for use by AS/400 TCP/IP to access the LAN.

If you do not have space for an additional LAN adapter, you may use indirect routing through the secure port of the firewall to access the AS/400 using the virtual LAN adapter. We do not recommend this because it increases the workload on the firewall.

We recommend that you specify a value of **none* in the `PORT1` and `PORT2` keywords of the `INSWNTSVR` command. This prevents line descriptions from being built for these ports on the AS/400 system.

Internal LAN addresses (Virtual LAN)

The internal LAN is a component of the Integrated Netfinity Server that enables the Windows NT server to talk to the AS/400 system internally, over the system bus, using TCP/IP.

The internal LAN uses Class B restricted Internet addresses for private domains. Therefore, the addresses are not propagated through Internet gateways or routers. You need to check whether your intranet uses these IP addresses already. These addresses are in the format 192.168.xxx.yyy, where xxx is the hardware resource number of the Integrated Netfinity Server. If so, the IP addresses that are automatically configured for the internal LAN may conflict with addresses on the external LAN, with potentially serious consequences. You can override the default assignment of IP addresses for the AS/400 and Windows NT ends of the internal LAN by entering addresses in the Internal LAN port parameter of the Install Windows NT Server (`INSWNTSVR`) command.

Alternatively, if you do have an address conflict, or want to change the IP addresses on the internal LAN for any reason, you can do this manually.

We recommend that you use the default addresses unless there is the possibility of a conflict.

AS/400 NetServer

To enable the application of AS/400 integration service packs to the Windows NT Server, the AS/400 NetServer function needs to be configured before starting the installation. You are instructed when to do this as you work through the installation chapter.

Installation source directory

Starting with Version 4 Release 4, you can install the Windows NT server from the AS/400 integrated file system (IFS), instead of a CD-ROM. This may be useful when you need to create multiple Windows NT servers on a single AS/400 system, or send an image of the installation CD-ROM to a remote location. We recommend that you install from the CD-ROM, unless you have a good reason to copy the image to the IFS.

Machine pool size

The following list shows the required additional memory in the AS/400 system machine pool for each Integrated Netfinity Server, depending on the type:

- Each Model 6617 or 6618 (SPD bus) Integrated Netfinity Server requires an additional 5.4 MB memory in the machine pool.
- Each Model 2852/2854/2857/2865/2866/2868 (PCI bus) Integrated Netfinity Server requires an additional 1.8 MB memory in the machine pool, in addition to 1.8 MB for each LAN adapter.

If the machine pool is not large enough, the network server may not become active.

We recommend that you change the performance adjustment system value (QPFRADJ) to automatically adjust the size of the machine pool, and then change it back (if necessary) after you have installed the server and brought it up. You are instructed when to do this during installation.

Program temporary fixes (PTFs)

PTFs are required for the following products:

- 5769-SS1 (option 29), OS/400 - AS/400 Integration for NT

Install the latest PTFs for the integration software. You can obtain this information from the Web at: <http://www.as400.ibm.com/nt>

Select **Service Information**, and then select **AS/400 PTF Descriptions**.

- 333 MHz Integrated Netfinity Server

If you are running Version 4 Release 2 or Version 4 Release 3 of OS/400, and have a 333 MHz Integrated Netfinity Server installed, you *must* install the PTFs to provide the required support.

We *strongly* recommend that you spend the time to compile a list of PTFs for your level of OS/400 and Integrated Netfinity Server hardware, and get them well in advance of your installation date. Most problems that arise during installation are due to missing PTFs.

Microsoft Windows NT Server Service Packs

Get the latest service pack for the integration software. IBM eNetwork Firewall for Windows NT requires service pack 4 or later. You can get this information from the Web site: <http://www.as400.ibm.com/nt>

Select **Service Information** and then **Service Packs**.

We *strongly* recommend that you order the latest Service Pack on CD-ROM well in advance of your installation date. Most problems that arise after installation are due to missing service packs.

AS/400 authorities

Verify that you have access to a user profile with the necessary authority to perform the installation. To set up Windows NT Server on an Integrated Netfinity Server, you must have *IOSYSCFG, *ALLOBJ, and *JOBCTL special authorities.

An administrator-level profile with *SECADM special authority is required to set up AS/400 NetServer.

Integrated Netfinity Server resource names

If you have *multiple* Integrated Netfinity Servers of the same type installed in your AS/400 system, you may not be able to tell them apart in the Display Communication Resources screen. You need this information to run the installation program.

To find out the physical Integrated Netfinity Server adapter to which a particular resource name refers, follow these steps:

1. If you are not already at the Display Communication Resources screen, type `DSPHDWRSC *CMN`, and then press Enter.
2. Type 7 in the Opt field to the left of the resource name for a File Server IOA or File Server IOP. The Display Resource Detail screen appears.
3. Look at the Card Position under the Physical Location column.
4. Look at the labels on the actual slots in your AS/400 system. One slot should be labeled with the same number or combination of letters and numbers shown in the Card Position field. This slot contains the Integrated Netfinity Server adapter to which the resource name refers.

Logical Partitioning (LPAR)

If you use logical partitions on your AS/400 system, install the IBM-supplied integration software (OS/400 option 29) on each logical partition where you are installing Windows NT Server. There is no requirement to install option 29 on all the logical partitions. For example, you can have one logical partition that has option 29, and one or more Windows NT Servers installed, and another logical partition that has neither option 29 nor any Windows NT Servers installed. You need to install Windows NT Server only on the logical partition that you use to vary the server on.

If you are going to use the AS/400 tape and CD-ROM drives from Windows NT running on the Integrated Netfinity Server, these devices must be assigned to the same logical partition as the Integrated Netfinity Server. Typically, if you are implementing logical partitioning, you will have multiple CD-ROM and tape drives on your AS/400 system because partitions are, in effect, separate AS/400 systems running on the same hardware.

8.3 Windows NT planning

Before installing Windows NT Server on the Integrated Netfinity Server, you must plan for the Windows NT-related items discussed in the following section.

Disk storage requirements

Sizing the disk storage requirements for your IBM eNetwork Firewall for Windows NT is the same for a Windows NT Server running on the Integrated Netfinity Server as it is for a Windows NT Server running on a PC. However, the Integrated Netfinity Server implementation may allow you more flexibility in terms of drive sizes (up to 8000 MB).

Refer to 8.4, “Disk storage sizing considerations” on page 294, for advice on estimating your disk storage requirements.

Memory sizing

Use the same guidelines for sizing memory on an Integrated Netfinity Server running Windows NT Server 4.0 as you would for sizing a PC-based 200 MHz or 333 MHz Pentium server.

A minimum of 64 MB of memory is required on the Integrated Netfinity Server to run Windows NT. However, you should consult the Microsoft guidelines for sizing memory on your Windows NT Server before you order the hardware.

We recommend that you order a minimum of 256 MB memory on your Integrated Netfinity Server.

Server Console

IBM does not supply a PC monitor, keyboard, or mouse as part of the Integrated Netfinity Server package. However, extension cables for the monitor, keyboard, and mouse are supplied.

IBM eNetwork Firewall for Windows NT requires a display that is capable of at least 1024 x 768 resolution.

Diskette drive

Because the Integrated Netfinity Server does not have a diskette drive, the software for installing Windows NT Server on the Integrated Netfinity Server is written so that a diskette is not required.

We recommend that, if you need a diskette drive to install other software on the Windows NT Server, use a drive that has been shared by another Windows workstation on the network. Or, obtain a drive that can be connected to the parallel port on the Integrated Netfinity Server.

CD-ROM drive

By default, the CD-ROM drive uses the first available drive letter after the last assigned drive letter. For example, if you create and link a user storage space to the server, the new disk may show up as drive F: in the Windows NT Disk Administrator. By default, the CD-ROM drive appears as drive G:. Therefore, you need to decide on a specific drive letter to assign to the CD-ROM drive so that it does not change every time you link a new storage space.

We recommend that you assign the drive letter X: to the CD-ROM drive.

Administrator password

During the Windows NT phase of the installation, you must assign a password to the Windows NT Administrator account. You should decide on a password when you complete the installation worksheet, write it down, and store it in a safe place.

Upgrade versions of Windows NT Server

If you are using an upgrade version of the Windows NT Server CD-ROM for the installation, Windows NT prompts you to insert a non-upgrade version to verify the license. Therefore, make sure you have the original licensed version on hand before you start the installation.

8.4 Disk storage sizing considerations

The installation of Windows NT on an Integrated Netfinity Server creates three storage spaces that represent the Windows NT C:, D:, and E: drives. The C: drive (DOS Boot) is small (only 10 MB) and is not discussed here. The D: drive holds an image of the Windows NT installation files. The Windows NT system is installed on the E: drive.

It is important that you accurately estimate the amount of disk storage that you require before you begin the installation.

Windows NT Server D: and E: drives

When using IBM eNetwork Firewall for Windows NT, the default sizes for the D: drive (200 MB) and E: drive (500 MB) are too small. In our test case, we defined a 2000 MB E: drive. Our Integrated Netfinity Server had 512 MB of memory installed. After all the products were installed and configured, we had 1.2GB of free space on the E: drive. Refer to "Windows NT virtual storage file (pagefile)" on page 295, for more information on how the amount of memory installed on the Integrated Netfinity Server affects the size of the E: drive. The log files, mail queues, and other files use space on the E: drive in a production environment. You should plan to allow space for growth of these items.

The D: drive can be from 200 to 1007 MB in size, and the E: drive can be from 500 MB to 8000 MB in size (up from 1007 MB in Version 4 Release 3). Notice that the larger E: drive capability is being made available on Version 4 Releases 2 and 3 via PTF.

If you specify a size of 1008 MB or greater for your E: drive, it is automatically created as a user storage space, rather than a system storage space. If you specify a size of 2048 MB (2 GB) or greater, the E: drive must be formatted as NT File System (NTFS).

IBM eNetwork Firewall for Windows NT requires the use of NTFS format for the E: drive.

You can increase the size of the E: drive after installation, but *only* if it has been created as a user storage space (1008 MB or greater). This information is contained in *AS/400 - Implementing Windows NT on the Integrated Netfinity Server*, SG24-2164. Notice that you *cannot* enlarge the C: or D: drives.

Enlarging the E: drive

User storage spaces of 1023 MB or less can only be copied to a storage space with a maximum size of 1023 MB. In other words, you cannot enlarge a user storage space of 1023 MB or less, beyond 1023 MB. User storage spaces of 1024 MB or more can be copied to another storage space of up to 8000 MB.

This is a limitation caused by the physical disk geometry.

We recommend that you specify the following minimum sizes for the D: and E: drives when installing Windows NT Server 4.0 and IBM eNetwork Firewall for Windows NT:

- D: drive: 200 MB
- E: drive: 1024 MB

This gives you the flexibility to enlarge the E: drive later (if necessary), and store some applications and files on the system drive.

These figures are suggested *minimum* requirements. You should carefully evaluate your disk storage requirements for both drives *before* installation.

Windows NT virtual storage file (pagefile)

Windows NT creates a virtual memory paging file (pagefile.sys) on the system drive (E:, in the case of Windows NT running on the Integrated Netfinity Server). This file is used to handle the swapping of data in and out of memory, as well as being used as a temporary dump file for STOP (blue screen) errors.

Windows NT calculates the size of the page file based on the amount of memory installed on the Integrated Netfinity Server. For example, on a 256 MB Integrated Netfinity Server, Windows NT creates a paging file with a minimum initial size of 256 MB and a maximum size of 306 MB. The more memory that is installed on your Integrated Netfinity Server, the greater the amount of disk space you should reserve on your E: drive. The reason is that Windows NT creates the page file in proportion to the amount of memory installed.

As a rule, for a Windows NT Server, you should allow 120% of the installed memory size on the Integrated Netfinity Server as additional disk storage on the E: drive for the page file.

We recommend that you allow enough space on the Windows NT system drive (E:) to comfortably accommodate the page file, because this is where it normally resides.

Microsoft Windows NT Service Packs

When you install a Windows NT service pack, you can specify whether you want to allow the un-install option. If you select the option to enable the un-install function, you should allow extra disk space. For Windows NT service pack 4, you need to allow approximately 40 MB.

8.5 Hardware and software checklists

Make sure that you have all the hardware and software that you need by checking off each item in the lists in the following sections.

Hardware checklist

Table 53 provides a checklist of the minimum hardware prerequisites that need to be installed on the AS/400 system before installing Windows NT Server on the Integrated Netfinity Server.

Table 53. Hardware checklist

Integrated Netfinity Server adapter installed in your AS/400 system	
Two LAN adapters installed for the Integrated Netfinity Server	
VGA or SVGA PC monitor connected to the Integrated Netfinity Server	
Keyboard connected to the Integrated Netfinity Server	
Mouse connected to the Integrated Netfinity Server	
LAN adapters in the Integrated Netfinity Server connected to the LAN	
At least 1 GB of disk space available for installation	

Software checklist

Table 54 provides a checklist of the minimum software requirements needed to complete the installation of Windows NT Server on an Integrated Netfinity Server.

Table 54. Software checklist

OS/400 Version 4 Release 2 (5769-SS1) or later release	
OS/400 Version 4 Release 2 (5769-SS1), or later release, option 29 - OS/400 - AS/400 Integration for NT	
The AS/400 PTFs specified at the Web site: http://www.as400.ibm.com/nt under Service Information->AS/400 PTF Descriptions	
The AS/400 Integration with Windows NT Server service packs specified at the Web site: http://www.as400.ibm.com/nt under Service Information ->Service Packs	
AS/400 Operations Navigator installed on an AS/400-connected PC ¹	
OS/400 Version 4 Release 2 (5769-SS1), or later release, option 12 - Host servers ²	
Windows NT Server 4.0 on CD-ROM or copied to the IFS	
License CD-ROM if installing from an upgrade CD-ROM	
Windows NT service pack 4 or later from Microsoft	
<p>1. AS/400 Operations Navigator is optional, and is shipped free of charge with OS/400 Version 4 Release 2 and later releases. It is required if you want to set up AS/400 NetServer or AS/400 DNS server. IBM eNetwork Firewall for Windows NT requires a DNS server in the secure network.</p> <p>2. Host Servers is a prerequisite for AS/400 Client Access and AS/400 NetServer printer support. Therefore, it is optional.</p>	

8.6 Installation worksheets

The worksheets presented in the following sections are designed to help you collect the necessary information to install Windows NT Server on the Integrated Netfinity Server. Make sure that you have all of the worksheets completed before you start the installation. The first worksheet (Table 55 on page 297) is used to complete the Install Windows NT Server (INSWNTSVR) command. It follows the layout of the command as closely as possible. This is the command that is used to start the installation process.

The second worksheet (Table 56 on page 301) is used when you define the TCP/IP interface configuration during the Windows NT Server configuration and during IBM eNetwork Firewall for Windows NT configuration.

The term *port*, used in the worksheet, refers to the LAN adapter or adapters (Token-Ring or Ethernet) installed with the Integrated Netfinity Server.

Sometimes it is not obvious as to which system a parameter applies. The values in *italic* (*AS/400 system*, *Windows NT*) shown in the *Parameter* column in Table 55 refer to whether a particular parameter applies to the AS/400 system, Windows NT, or both.

Table 55. Installation worksheet to support firewalls on the Integrated Netfinity Server

Parameter	Description	Value
Network server description <i>AS/400 system</i> <i>Windows NT</i>	Specifies the name of the network server. It can be up to eight characters in length. This name is used as the name of the AS/400 network server description, the Windows NT computer name, and the Windows NT Server TCP/IP host name. It is used as the basis for the names of other components.	
Resource name <i>AS/400 system</i>	Specifies the hardware resource name that the network server description uses. Use the Work With Hardware Resources (<code>WRKHDWRSC *CMN</code>) command to determine the resource name. If you have an Integrated Netfinity Server model 28xx (PCI), look for a name with format LINxx. On a model 6617 or 6618 (SPD), look for a name with format CCxx. The text associated with the resource name contains File Server IOA (PCI) or File Server IOP (SPD).	
Domain Role <i>Windows NT</i>	Specifies the role being performed by this network server. For a network server that supports IBM eNetwork Firewall for Windows NT, you <i>must</i> select *SERVER .	*SERVER
Windows NT version <i>Windows NT</i>	Specifies the version of Windows NT to install on this network server. At the time this redbook was written, you must set this parameter to the default *NT4.0. However, in the future, this parameter will allow you to install later versions of Windows NT Server, other than 4.0.	

Parameter	Description	Value
Windows NT source directory <i>AS/400 system</i>	Specifies the path name of the Integrated File System directory that contains the Windows NT CD-ROM image that is used as the source for the install. *DFT Causes the installation program to read from the CD-ROM drive. This is the default. The directory name may reference an optical volume ('/QOPT/volume'), a folder ('/QDLS/folder'), or another IFS directory ('/dir1/dir2').	
Install option <i>Windows NT</i>	Specifies the Windows NT installation method. At the time this redbook was written, you must set this parameter to the default. *INSTALL.*REINSTALL is not used in Version 4 Release 4, so do not specify it.	
Port 1 Port 2 <i>AS/400 System</i>	Specifies the ports of the Integrated Netfinity Server that are used by the AS/400 system.	*NONE
TCP/IP local domain name <i>Windows NT</i>	Specifies the TCP/IP domain name associated with the Windows NT server. The case is maintained as it is entered, and the case is significant. Enter *SYS to use the same domain name that the AS/400 system uses.	
TCP/IP name server system <i>Windows NT</i>	Specifies the TCP/IP address of the domain name server or servers to be used by Windows NT. This is the IP address used by the firewall to resolve IP addresses on the Internet.	
Server message queue and library <i>AS/400 system</i>	Optionally specifies a message queue and library. We recommend that you specify a message queue. If the message queue does not exist, it is created. If you specify a name and library for a message queue, this queue receives messages issued by the server, as well as informational messages, and messages requiring operator intervention. Optionally, it receives Windows NT Event Log messages. The message queue should be monitored so that it does not become full. If it becomes full, messages are rerouted to the job log of the user administration monitor job. Take care if QSYSOPR is specified, because the volume of Windows NT event log messages is unpredictable. *JOBLOG Places Windows NT event log messages from the server, and informational messages on the job log of the user administration monitor job. Errors requiring operator intervention are sent to the QSYSOPR message queue. *NONE Windows NT event log messages and informational messages are not placed on any message queue. However, errors requiring operator intervention are sent to the QSYSOPR message queue.	

Parameter	Description	Value
Event log <i>AS/400</i>	<p>Specifies the type of Windows NT Event Log messages that are mirrored to the AS/400 server message queue, as specified in the previous parameter.</p> <p>The Windows NT Event Log is the central repository for error reporting on Windows NT and consists of system (*SYS), security (*SEC), and application (*APP) messages. The default is to monitor all three message types (*ALL). However, you can choose to mirror a combination of these message types to the server's message queue, or none (*NONE) of them.</p> <p>You can change the level of message logging on the AS/400 system at a later time, if necessary, using the Change Network Server Description (CHGNWSD) command. Notice that, if the security log is mirrored, be sure to set up the message queue with an appropriate level of security because the status of user logons and password changes may appear in the log.</p>	
Server storage space sizes <i>AS/400 system Windows NT</i>	<p>Specifies the size of the following Windows NT drives:</p> <ul style="list-style-type: none"> - Install source drive (D:): 200 - 1007 MB - System drive (E:): 500 - 8000 MB <p>Carefully consider how large to make these drives. While E: drives greater than 1023 MB can be enlarged later, the D: drive cannot. Refer to Section 8.4, "Disk storage sizing considerations" on page 294, for a discussion of drive sizing.</p>	
Convert to NTFS <i>Windows NT</i>	<p>Specifies whether you want the E: drive to be formatted as FAT or NTFS.</p> <p>To support the firewall, you must format the E: drive as NTFS (*YES) . This provides improved performance and enhanced security provided by NTFS permissions.</p>	*YES
To workgroup <i>Windows NT</i>	<p>Specifies the name of the Windows NT workgroup in which this server participates.</p> <p>If you do not specify a value here, Windows NT prompts for a value later during the installation. A member server can be part of either a domain or a workgroup. This parameter only appears if you specify a domain role of *SERVER.</p>	
Full name and organization <i>Windows NT</i>	<p>Specifies the full name of the individual and organization that holds the Windows NT Server license.</p> <p>If you do not specify a value here, Windows NT prompts for a value later during the installation.</p>	
Language version <i>AS/400 system</i>	<p>Specifies the primary language used to display AS/400 Integration with Windows NT Server text and messages. *PRIMARY is the default.</p> <p>This value should correspond to the language version of Windows NT Server that is going to be used on the Integrated Netfinity Server. It is also used to determine a predefined list of names that are reserved as user profiles in Windows NT (for example, Administrator and Guest, in the English version).</p>	
Synchronize date and time <i>Windows NT</i>	<p>Specifies when the date and time are updated on the Windows NT Server from the AS/400 system.</p> <p>*YES Synchronizes the Windows NT Server time with the time of the AS/400 system during vary on, and then every 30 minutes.</p> <p>*NO Synchronizes the time only during vary on.</p> <p>We recommend the value *YES.</p>	

Parameter	Description	Value
Windows NT license key <i>Windows NT</i>	Specifies the license key which can be found on a sticker on the back of the installation CD case. If you do not specify a value here, Windows NT prompts for a value later during the installation. You need to enter the key exactly as printed on the case. Make sure you include any dashes. Otherwise, the value you enter is ignored and Windows NT prompts for a value later during the installation.	
License mode <i>Windows NT</i>	Specifies whether Windows NT is installed in a per seat or per server license mode. *PERSEAT Client licenses have been purchased for each computer that accesses the server, separate from the server license. *PERSERVER A certain number of client licenses have been purchased with the server license. The number of client licenses purchased with the server license must also be specified in the Client licenses parameter. The Client licenses parameter is valid only when License mode *PERSERVER is specified.	
Restricted device resources <i>AS/400 system</i> <i>Windows NT</i>	Specifies which AS/400 tape and CD-ROM drives are <i>not</i> accessible from Windows NT running on the Integrated Netfinity Server. This parameter enables you to restrict which AS/400 tape drives are used to backup Windows NT data, when using a Windows NT backup application, such as the Windows NT Backup Utility or Seagate Backup Exec. This parameter does not affect which tape drives can be used to back up Windows NT data from the AS/400 side. *NONE Specifies that all AS/400 tape and CD-ROM drives can be used by the server. This is the default. *ALL Specifies that no AS/400 tape or optical drives can be used by the server. *ALLTAPE Specifies that no AS/400 tape drives are used by the server. *ALLOPT Specifies that no AS/400 CD-ROM drives are used by the server. You can specify a list of up to ten device names that cannot be used by the server. We recommend the value *NONE for this parameter.	
Text 'description' <i>AS/400 system</i>	Specifies the text that briefly describes the network server description created by this command (up to 50 characters).	
Keyboard layout <i>Windows NT</i>	Specifies the keyboard layout identifier to install on the Windows NT Server. Press F10 to see this parameter. If you want to install a keyboard type on the Windows NT Server other than the default, specify the keyboard layout identifier in the Keyboard layout field. Valid keyboard layout identifiers are listed in the TXTSETUP.SIF file in the i386 directory of the Windows NT installation source.	

Parameter	Description	Value
Internal LAN port <i>AS/400 system</i> <i>Windows NT</i>	<p>Specifies the IP addresses for the AS/400 and Windows NT ends of the internal LAN. (Press F10 to see this parameter.)</p> <p>*GEN Causes the IP addresses to be automatically generated. This is the default.</p> <p>If you decide to specify IP addresses for the AS/400 and Windows NT sides of the internal LAN, they override system-generated ones. To avoid potential conflicts, you can specify override IP addresses that you know are unique across your network. Use addresses of the form a.b.x.y, where a.b.x is the same value for both sides of the internal LAN, and ensure that the internal LAN occupies its own subnet on the AS/400 system. We recommend the value *GEN for this parameter.</p>	AS/400 Windows NT
Configuration file <i>Windows NT</i>	<p>Specifies the name of a source file containing configuration data used in activating or further defining the server. Press F10 to see this parameter.</p> <p>*NONE The default. Indicates that no configuration file is specified.</p> <p>If you have a customized configuration file, specify it here together with the name of the library where it is stored (*LIBL, *CURLIB, or the name of the library).</p>	

Refer to Table 56 to help you define the TCP/IP interface configuration.

Table 56. Interface worksheet

Interface number	Interface type (circle type)	IP address	Subnet mask
1	Secure / Non-Secure		
2	Secure / Non-Secure		
3 (*INTERNAL)	Secure / Non-Secure		

8.6.1 SPD packaging

The SPD version contains one book package with three slots for PCI LAN adapters. This package requires three slots in the AS/400 system. Figure 350 on page 302 shows the packaging of the SPD version of the Integrated Netfinity Server adapter.

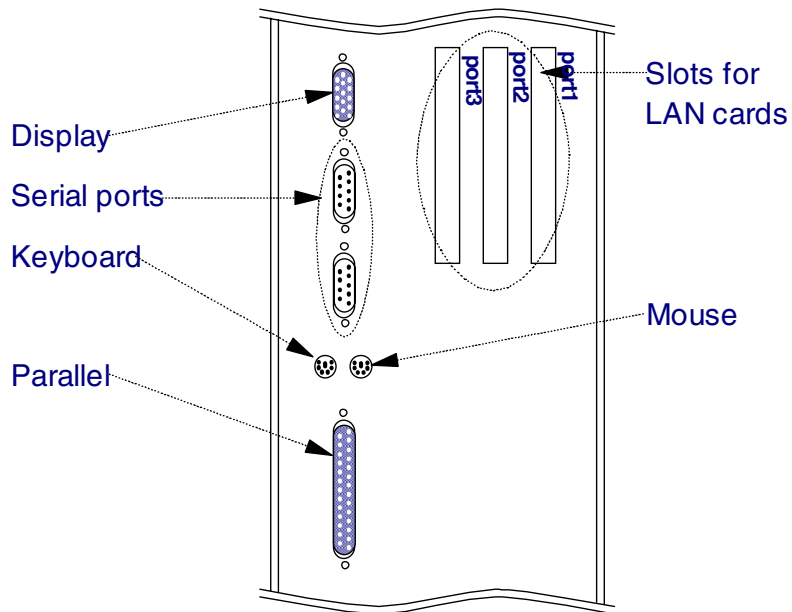


Figure 350. Integrated Netfinity Server SPD packaging

A display port, two serial ports, a keyboard port, a mouse port, and a parallel port are on the left side of the card. There are three PCI slots for LAN cards, but there are restrictions on how these adapters can be used.

8.6.2 PCI packaging

The PCI version contains the following parts:

- A processor card
- A bridge card with attached port box cable
- Up to two PCI LAN adapters

The processor and bridge cards need two PCI slots in the AS/400 system. In addition, one or two PCI slots are required for LAN adapters, which fit in the slots reserved for this purpose in PCI-based AS/400 systems

Figure 351 on page 303 shows the packaging of the PCI based Integrated Netfinity Server. You can see a bridge card to which the port box cable, display cable, and two LAN cards (if they are installed) are connected.

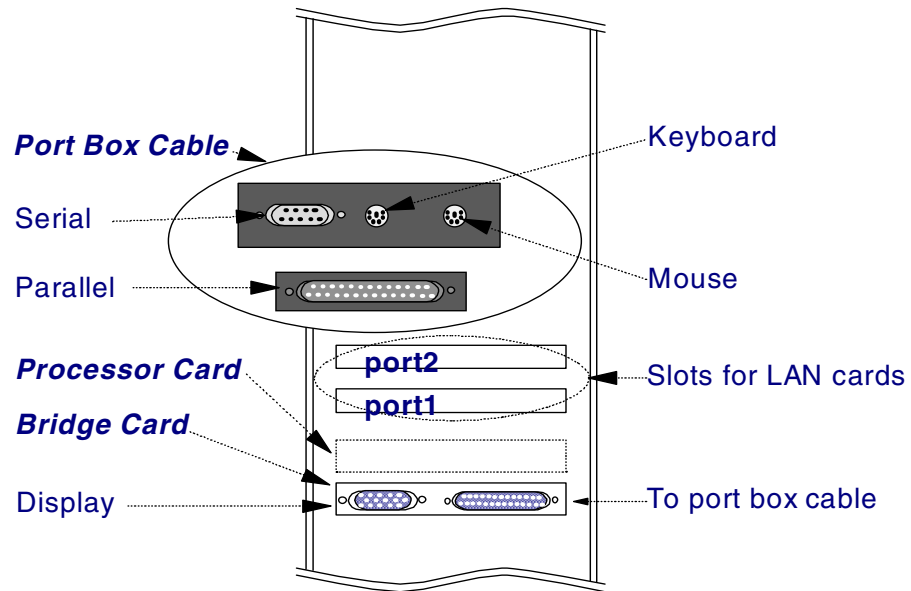


Figure 351. Integrated Netfinity Server PCI packaging

8.6.3 Installation steps

The installation of Windows NT Server on an Integrated Netfinity Server consists of the following main steps:

1. Completing the pre-installation tasks
2. Starting the Windows NT server installation from the AS/400 system
3. Completing the Windows NT Server installation from the Windows NT console
4. Completing the post-installation tasks

Each of these steps is described in the following sections. Before you begin, make sure the installation worksheet is complete.

8.7 Completing the pre-installation tasks

Before you can start installing Windows NT on an Integrated Netfinity Server, you need to complete the following pre-installation tasks:

1. Install the integration software.

Make sure that the integration software is installed on the AS/400 system. Follow these steps:

- a. Type `GO LICPGM` on a command line, and press Enter.
- b. Select option **10** to display the installed programs, and press Enter.
- c. Look for **OS/400 - AS/400 Integration for NT** (5769-SS1, option 29). If you cannot find it, continue with the next step.
- d. Insert the CD-ROM containing the integration software into the AS/400 system CD-ROM drive.
- e. Return to the Work with Licensed Programs (`GO LICPGM`) menu. Select option **11** (Install Licensed Programs), and press Enter.

- f. Page down until you find the entry **OS/400 - AS/400 Integration for NT**. Type 1 in the Option column, and press Enter.
- g. Type the correct device name for your CD-ROM drive (typically OPT01), and press Enter.
- h. After installing the new software on your AS/400 system, install the latest cumulative PTF tape to update the new software.

2. Install the PTFs.

Most errors that occur during and after installation can be traced back to the fact that code updates have not been installed. Before you attempt to install Windows NT Server on the Integrated Netfinity Server, make sure that you install all the required PTFs on your AS/400 system. Failure to do so may result in errors either during or after installation.

Notice that, at the end of the installation process, the Level Check program automatically prompts you to download any integration service packs that are installed on your AS/400 system to the Windows NT Server.

3. Set the performance adjustment (QPRFADJ) system value.

To vary on the Integrated Netfinity Server, there must be enough memory in the machine pool. Rather than calculating how much more memory you need and then manually adjusting the machine pool size, we suggest that you turn on automatic performance adjustment. To change the QPRFADJ system value, follow these steps:

- a. Type `WRKSYSVAL SYSVAL(QPRFADJ)` on a command line, and press Enter.
- b. Type 2 in the Option column, and press Enter.
- c. Change the QPRFADJ system value to 2. This is the default.

4. Set the coordinated universal time offset (QUTCOFFSET) system value.

To ensure that time synchronization between the AS/400 system and Windows NT Server works, verify that the QUTCOFFSET system value is correctly set on the AS/400 system using the `WRKSYSVAL QUTCOFFSET` command.

If you do not know what the offset for your time zone is, you can determine this by going to a Windows 95, 98, or NT workstation. Click on **Start->Settings->Control Panel->Date/Time->Time Zone**. Click on the down arrow and find the correct offset for your region. Then, go back and set it on the AS/400 system. Do not forget to include the preceding + or - symbol.

5. Enable the AS/400 NetServer support.

For integration software service packs to be installed on Windows NT, support for Windows Network Neighborhood must be enabled on the AS/400 system. This should be done before installation is started to allow automatic download of any existing integration service packs when the installation process finishes.

6. Configure TCP/IP on the AS/400 system.

The installation program allows you to automatically pass the AS/400 TCP/IP configuration data across to Windows NT, which are the TCP/IP local domain name and the Domain Name Server (DNS) IP addresses.

If you intend to use this feature, make sure that a local domain name and one or more Domain Name Servers are configured on the AS/400 system. Use the Configure TCP/IP (`CFGTCP`) command to check this.

If you have never set up TCP/IP on your AS/400 system, you do not need to use this feature. In fact, you do not have to configure anything concerning TCP/IP on your AS/400 system. The Install Windows NT Server (`INSWNTSVR`) command creates the necessary TCP/IP interfaces on the AS/400 system. Also, TCP/IP is started automatically when the Integrated Netfinity Server is varied on using the Vary Configuration (`VRFCFG`) command.

There are some network configuration parameters that are *not* automatically passed across from the AS/400 system or specified in the `INSWNTSVR` command.

The gateway address attributes are included. If the AS/400 system and Windows NT server are on the same TCP/IP subnet, you can determine the gateway IP address from the AS/400 system. Type `CFGTCP` on a command line. Select option **2**. Otherwise, you need to ask your network administrator.

For more information regarding TCP/IP configuration on the AS/400 system, refer to *TCP/IP Configuration and Reference*, SC41-5420.

7. Create drive E: in a user ASP.

If you make your Windows NT system drive E: 1,008 MB or larger, the AS/400 system creates the drive as a user storage space in the system auxiliary storage pool (ASP 1) by default. You can have the AS/400 system create the drive in a user auxiliary storage pool (ASP) instead. To do this, create a data area called QNTAPNWS in the QUSRSYS library before running the Install Windows NT Server (`INSWNTSVR`) command. For example, at the AS/400 command line, type the following command, where `n` is the user ASP number ranging from 2 through 16:

```
CRDTAARA DTAARA(QUSRSYS/QNTAPNWS) TYPE(*DEC) LEN(4 0) VALUE(n)
```

8.8 Starting the Windows NT Server installation from the AS/400 system

We are now ready to start the AS/400 part of the Windows NT installation. Make sure you have filled out the worksheet so that you have all the necessary information right in front of you. Table 57 on page 306 is our sample worksheet.

Also, make sure you are signed on to the AS/400 system with a profile that has `*IOSYSCFG`, `*ALLOBJ`, and `*SECADM` special authorities.

Note: Be aware that during this long running command, the Integrated Netfinity Server may be varied off and on several times.

Table 57. Installation worksheet used in our Integrated Netfinity Server configuration

Parameter	Description	Value
Network server description	Specifies the name of the network server. It can be up to eight characters in length.	NTFIREWL
Resource name	Specifies the hardware resource name that the network server description uses.	LIN02
Domain Role	Specifies the role being performed by this network server.	*SERVER
Windows NT version	Specifies the version of Windows NT to install on this network server.	*NT40
Windows NT source directory	Specifies the path name of the Integrated File System directory that contains the Windows NT CD-ROM image that is used as the source for the installation.	*DFT
Install option	Specifies the Windows NT installation method.	*INSTALL
Port 1 Port 2	Specifies the ports of the Integrated Netfinity Server that are used by the AS/400 system.	*NONE
TCP/IP local domain name	Specifies the TCP/IP domain name associated with the Windows NT server. The case is maintained as it is entered, and the case is significant.	*SYS
TCP/IP name server system	Specifies the TCP/IP address of the Domain Name Server or servers to be used by Windows NT.	208.123.5.4
Server message queue and library	Optionally specifies a message queue and library.	NTFWMSGQ
Event log	Specifies the type of Windows NT event log messages that are mirrored to the AS/400 server message queue, as specified in the previous parameter.	*ALL
Server storage space sizes	Specifies the size of the following Windows NT drives: - Install source drive (D:): 200 - 1007 MB - System drive (E:): 500 - 8000 MB	D: 200 E: 2000
Convert to NTFS	Specifies whether you want the E: drive to be formatted as FAT or NTFS.	*YES
To workgroup	Specifies the name of the Windows NT workgroup in which this server participates.	KEEPOUT
Full name and organization	Specifies the full name of the individual and organization that holds the Windows NT Server license.	IBM ITSO
Language version	Specifies the primary language used to display AS/400 Integration with Windows NT Server text and messages. *PRIMARY is the default.	*PRIMARY
Synchronize date and time	Specifies when the date and time are updated on the Windows NT Server from the AS/400 system.	*YES
Windows NT license key	Specifies the license key which can be found on a sticker on the back of the installation CD case.	nnn-nnnnnnn
License mode	Specifies whether Windows NT is installed in a per seat or per server license mode.	*PERSEAT
Restricted device resources	Specifies which AS/400 tape and CD-ROM drives are <i>not</i> accessible from Windows NT running on the Integrated Netfinity Server.	*NONE
Text 'description'	Specifies the text that briefly describes the network server description created by this command (up to 50 characters).	NWS used for firewall

Table 58 shows our sample Interface worksheet.

Table 58. Interface worksheet used in our Integrated Netfinity Server configuration

Interface number	Interface type (circle type)	IP Address	Subnet Mask
1	Secure Non-Secure	10.1.1.2	255.0.0.0
2	Secure Non-Secure	208.222.150.250	255.255.255.248
3 (*internal)	Secure Non-Secure	Value from message	255.255.255.0

Perform these steps to create the network server to support IBM eNetwork Firewall for Windows NT:

1. Make sure the AS/400 CD-ROM drive is varied on. Insert the Windows NT Server 4.0 installation CD-ROM into the CD-ROM drive (if you are *not* installing from a directory in the IFS).
2. Type `INSWNTSVR` on an AS/400 command line, and press **F4**.
3. Type the information required to complete the first Install Windows NT Server (INSWNTSVR) display shown in Figure 352. Use the information from the worksheet you completed in Table 55 on page 297 (our sample values are shown in Figure 57 on page 306).

```

Install Windows NT Server (INSWNTSVR)

Type choices, press Enter.

Network server description . . . > NTFIREWL      Name
Resource name . . . . . > LIN02                Name
Domain role . . . . . > *SERVER                *DMNCTL, *BKUCTL, *SERVER
Windows NT version . . . . . *NT40             *NT40
Windows NT source directory . . *DFT

Install option . . . . . *INSTALL               *INSTALL
Port 1:
  Line type . . . . . *NONE                    *NONE, *ETH10M, *ETH100M...
  Local adapter address . . . . .                020000000000-7FFFFFFFFFFFF
  Maximum transmission unit . . 1492            Number
  AS/400 internet address . . . *NONE
  AS/400 subnet mask . . . . . *NONE
  NT internet address . . . . .
  NT subnet mask . . . . .

More...

```

Figure 352. INSWNTSVR display (Part 1 of 4)

4. Enter information from the worksheet into the second, third, and fourth displays of the Install Windows NT Server (INSWNTSVR) command. Examples are shown in Figure 353 through Figure 355 on the following pages.

```

                                Install Windows NT Server (INSWNTSVR)

Type choices, press Enter.

Port 2:
Line type . . . . . *NONE          *NONE, *ETH10M, *ETH100M...
Local adapter address . . . . .      020000000000-7FFFFFFFFFFFF
Maximum transmission unit . . . . . 1492      Number
AS/400 internet address . . . . . *NONE
AS/400 subnet mask . . . . . *NONE
NT internet address . . . . .
NT subnet mask . . . . .
TCP/IP local domain name . . . . . *SYS

TCP/IP name server system . . . . . 208.123.4.5
      + for more values
Server message queue . . . . . NTFWMSGQ      Name, *JOBLOG, *NONE
      Library . . . . . QUSRSYS      Name, *LIBL, *CURLIB
Event log . . . . . *ALL          *ALL, *NONE, *SYS, *SEC, *APP
      + for more values

More...

```

Figure 353. INSWNTSVR display (Part 2 of 4)

```

                                Install Windows NT Server (INSWNTSVR)

Type choices, press Enter.

Server storage space sizes:
Install source drive size . . . . . 200          200-1007
System drive size . . . . . 2000          500-8000
Convert to NTFS . . . . . *YES          *NO, *YES
To workgroup . . . . . KEEPOUT
To domain . . . . .
Full Name . . . . . IBM ITSO
Organization . . . . . IBM ITSO
Language version . . . . . *PRIMARY      *PRIMARY, 2911, 2922, 2923...
Synchronize date and time . . . . . *YES          *YES, *NO
Windows NT license key . . . . . nnn-mnnmnn
License mode:
License type . . . . . *PERSEAT      *PERSEAT, *PERSERVER
Client licenses . . . . .      Number
Restricted device resources . . . . . *NONE          Name, *NONE, *ALL...
      + for more values

More...

```

Figure 354. INSWNTSVR display (Part 3 of 4)

```

Install Windows NT Server (INSWNTSVR)

Type choices, press Enter.

Text 'description' . . . . . > 'NWS used for Firewall'

Additional Parameters

Keyboard layout . . . . . *DEFAULT      Hexadecimal value, *DEFAULT
Internal LAN port:
AS/400 internet address . . . *GEN
NT internet address . . . . . *GEN
Configuration file . . . . . *NONE      Name, *NONE
Library . . . . .                      Name, *LIBL, *CURLIB

```

Figure 355. INSWNTSVR display (Part 4 of 4)

5. Press Enter after you have completed the last display. The installation process starts (unless you made an error or omitted a mandatory parameter). The INSWNTSVR command performs the following tasks on the AS/400 system:
 - a. Creates the AS/400 line descriptions for the *internal Token-Ring line.
 - b. Creates the TCP/IP interface for the AS/400 end of the *internal (virtual) LAN.
 - c. Creates and formats the storage spaces that represent the C:, D:, and E: drives, and copies a minimal PC-DOS boot image to drive C:.
 - d. Creates the AS/400 network server description.
 - e. Copies the contents of the \i386 directory and its subdirectories from the Windows NT installation CD-ROM to the D: drive.
 - f. Copies programs, files, and device drivers specific to Windows NT running on the Integrated Netfinity Server to the D: drive into a directory named \i386\SOEM\$.
 - g. Creates an UNATTEND.TXT file that contains all the Windows NT-specific information entered in the INSWNTSVR command. It also allows for an almost unattended installation of Windows NT Server 4.0.
 - h. Starts TCP/IP on the AS/400 system, if it is not already active.
 - i. Varies on the network server description to start the DOS mini-boot image on drive C:.

The AUTOEXEC.BAT file on drive C: contains the necessary statement to kick off the unattended installation of Windows NT Server 4.0. If you watch the Windows NT Server console, you see the normal boot process of a PC, followed by DOS starting, and then the first phase of a Windows NT installation.
 - j. At the end of this phase of the installation, the generated IP address for the Windows NT end of the internal LAN is shown on the display from which the INSWNTSVR command was run.

See the following example:

Specify 192.168.xxx.xxx as the IP Address for the Virtual Token Ring Adapter

Write the address down here and in Table 56 on page 301.

Notice that you can also view this information in the job log of the installation job.

When this stage completes, the AS/400 system displays the message NTA100F First phase of install completed for server in the job log.

Job log

The INSWNTSVR command writes an extensive job log that contains information about any problems encountered during the installation. In the job log, you can find the IP address assigned to the Windows NT side of the virtual LAN. Make sure you save this job log after the installation is complete, because it can be used to diagnose any problems that are encountered during the installation process.

After the AS/400 part of the installation is complete, the network server description is varied on, TCP/IP on the AS/400 system is started (if it is not already active), and the actual Windows NT installation on the Integrated Netfinity Server starts. At this time, the console attached to the Integrated Netfinity Server starts. You can begin the next phase of the installation (refer to the following section).

8.9 Completing the installation from the Windows NT console

The AS/400 part of the installation created an UNATTEND.TXT file with all the Windows NT parameters you entered in the INSWNTSVR command. This UNATTEND.TXT file allows for an almost unattended installation of Windows NT. Detailed information about the Windows NT installation can be found in the appropriate Windows NT documentation available from Microsoft and other sources.

The installation of Windows NT Server on an Integrated PC Server is performed in the following four phases, called *modes*:

Mode 1 Character mode copies all files necessary to complete the setup process from the CD-ROM to a temporary directory and prepares the disk image for the next phase of the installation.

This phase is triggered by the INSWNTSVR command.

Mode 2 Text mode copies all files required for installation from the temporary directory to the installation directory.

This phase, and the following one, run on the Integrated Netfinity Server and are completely unattended.

Mode 3 Convert mode transforms the Windows NT installation partition from the default FAT format to the NTFS format if `CVNTFS (*YES)` was

specified in the INSWNTSVR command, or the size specified for the system drive in the INSWNTSVR command is greater than 2,047 MB.

Mode 4 This mode displays a graphical user interface (GUI), and prompts for additional information used to customize the Windows NT Server.

If the INSWNTSVR command fails before mode 4, the AS/400 system attempts to clean up and remove the following objects created during installation:

- Network server description (which deletes the server storage spaces as well)
- Any line descriptions that have been created
- TCP/IP interface for the internal LAN
- Message queue

Then, you must start the installation from the beginning. Before you attempt another installation, make sure all the objects are really deleted.

If the Install Windows NT Server (INSWNTSVR) command fails at the end of mode 4 (which is when the Integrated Netfinity Server is varied on, and Windows NT is started in GUI mode for the first time), the AS/400 side of the installation is complete. In this case, the AS/400 system does not attempt to clean up. All you must do is vary on the Integrated Netfinity Server, sign on to Windows NT, and complete the installation (if possible).

You do not need to take any action during the first three modes. However, in mode 4, you are prompted for the following input on the Windows NT console:

1. If you are using an upgrade version of Windows NT Server, and the installation program prompts you for a full license version, insert the full license CD-ROM, and press Enter to continue. If the installation program re-prompts you for the full license CD-ROM, press Enter again.
2. The Windows NT console should display the Microsoft License Agreement. Click **I agree**.
3. If you are installing your Windows NT Server as a primary domain controller, you are prompted to enter a password for the Windows NT Administrator. Write this password down and store it in a safe place, if you have not already done so.
4. Two error panels are displayed named **Error - Unattended Setup**. They inform you that the IP address and subnet mask are not valid. This is normal. Click **OK** on each one, and the panel shown in Figure 356 on page 312 appears. You are now ready to enter Windows NT Server TCP/IP network information.

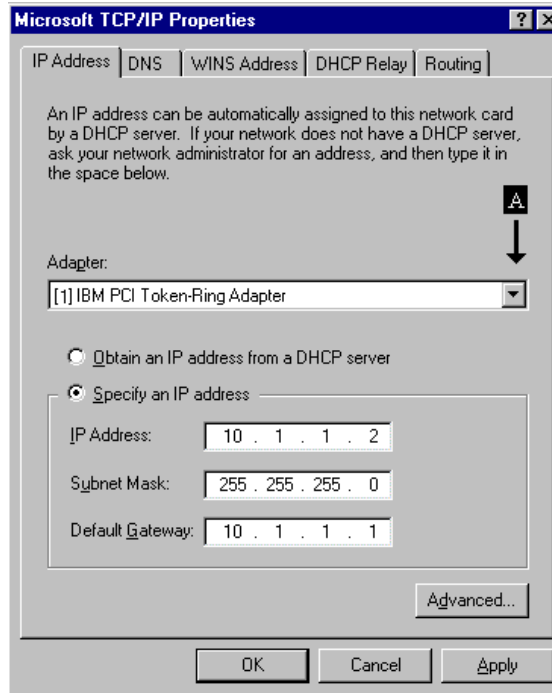


Figure 356. TCP/IP settings for a Token-Ring PCI adapter

Note: Please be aware that, at this point, you may have up to four LAN adapters to configure: the internal LAN (which is called the *AS/400 Virtual Token-Ring adapter*), in addition to one to three external LAN adapters representing the physical adapters under the control of the Integrated Netfinity Server. To configure adapter-specific parameters, you have to select the adapter from the pull-down list (A in Figure 356). The numbers in square brackets are the adapter numbers that Windows NT uses to differentiate the adapters.

Here is an example of the adapter names:

- [1] AMD PCNET PCI Ethernet Adapter
- [2] IBM PCI Token-Ring Adapter
- [3] AS/400 Virtual Token Ring Adapter

Because Windows NT Server uses autodetect to discover these adapters, the adapter number listed in the drop-down list *may not* correspond to the port numbers shown in Figure 350 on page 302 and Figure 351 on page 303. You must determine for certain which Windows NT Server adapter number matches the port number and cable on the AS/400 system unit. One way to determine this is to assign the TCP/IP address information to each adapter and then use the `PING` command to test the network connectivity of the interfaces. Refer to 8.10, “Determining the port to Windows NT Server adapter number” on page 316, for details.

5. From the Adapter pull-down menu (A in Figure 356 on page 312), select each of the *real* PCI LAN adapters attached to the Integrated Netfinity Server, one at a time, and fill in the following Windows NT information:
 - TCP/IP address
 - Subnet mask
 - Default gateway address or addresses (if applicable)

The TCP/IP address and subnet mask for the real adapters should be the same as the ones you recorded in the NT Internet address and NT subnet mask parameters of the installation worksheet in Table 56 on page 301 (our sample values are shown in Table 57 on page 306).

The last adapter listed is usually the AS/400 Virtual Token Ring Adapter. An example is shown in Figure 357. Proceed to the next step to configure this adapter.

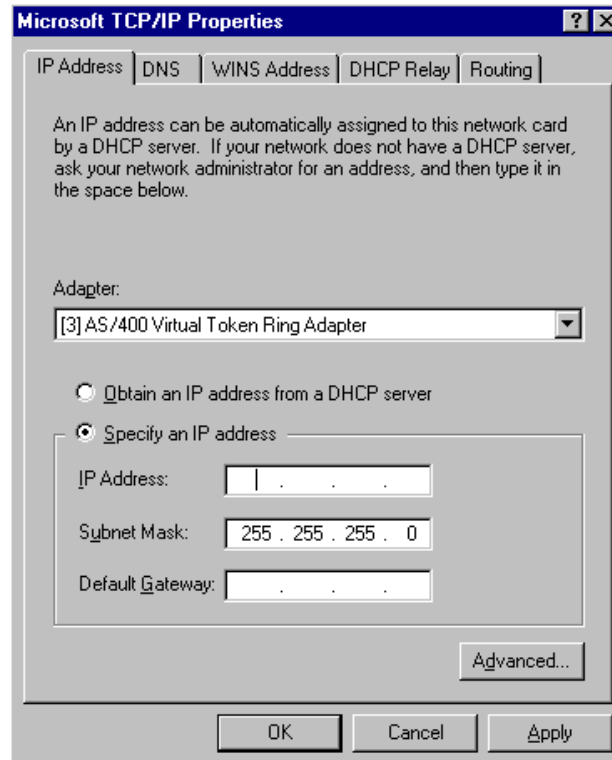


Figure 357. Enter TCP/IP address for the virtual LAN adapter

6. When the panel shown in Figure 357 is displayed, you need to enter the IP address for the AS/400 Virtual Token-Ring adapter that you recorded in step j. on page 309 of 8.8, “Starting the Windows NT Server installation from the AS/400 system” on page 305, in the IP address field.

The subnet mask is always 255.255.255.0. There is no default gateway address.

Note: Do *not* change these values.

7. After you complete the IP address information, click the **Routing** tab. If you are going to use Network Address Translation (NAT) or routing with your firewall, make sure **Enable IP Forwarding** is checked as shown in Figure 358 on page 314.

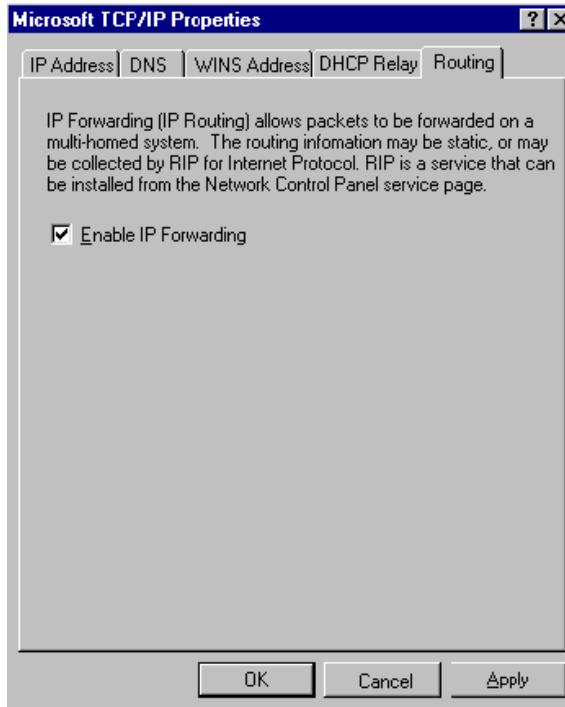


Figure 358. TCP/IP settings - Routing

8. Click **OK** to close the TCP/IP properties notebook.
If you are not using WINS, and receive an error about missing WINS addresses, click **Yes** to continue.
9. The AS/400 system does not automatically adjust for daylight savings time. To keep the AS/400 system and the Windows NT Server times synchronized, follow these steps:
 - a. Type `DSPSYSVAL SYSVAL (QUTCOFFSET)` on an AS/400 command line, and press Enter. This displays the coordinated universal time offset from UTC (Greenwich Mean Time). Record this value here: _____
 - b. On the Windows NT console, click **Date/Time** in the Control Panel, then select the **Time Zone** tab. Select the time zone from the drop-down list that matches the UTC offset recorded in the previous step. An example is shown in Figure 359 on page 315.

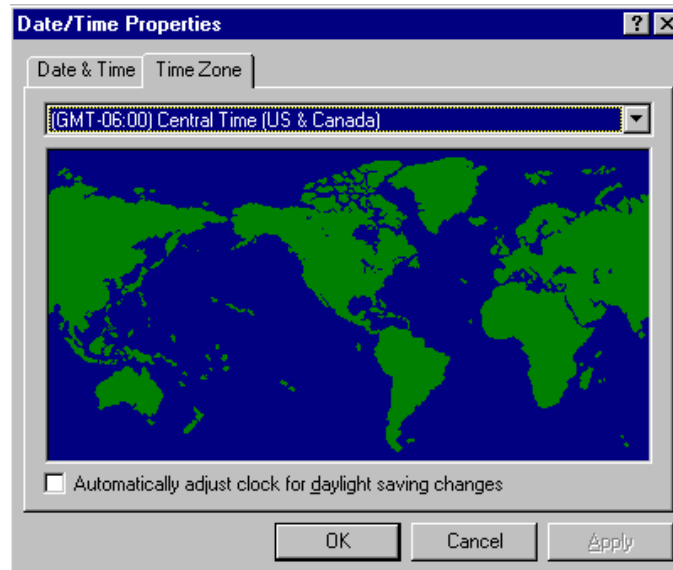


Figure 359. Setting the Windows NT Time Zone

- c. Remove the check from the Automatically adjust clock for daylight saving changes option. This forces AS/400 time and Windows NT time out of synchronization when the dates for switching to or from daylight savings time are reached.
- d. Click **Close**.

Notice that if you selected the option *YES for Synchronize date and time in the INSWNTSVR command, the AS/400 system synchronizes its time with the Windows NT Server every 30 minutes. If you selected *NO for the same option, the time is still synchronized, but only when the server is started.

10. The Windows NT Server completes the installation process, and then restarts. Some versions of Windows NT Server have additional automatic installation steps beyond those under the control of the INSWNTSVR command. These steps may cause additional installation phases and corresponding reboots of the Integrated Netfinity Server.

The basic installation of your Windows NT Server is now complete. The message Windows NT install source copied successfully appears.

Now that the installation of Windows NT Server on an Integrated PC Server is finished, print and read your job log. Check for any anomalies. We recommend that you keep the job log and installation worksheet for reference.

Time required

As a guide, the time required from the start of the INSWNTSVR command on the AS/400 system to this point is between 30 minutes and 1 hour. Your time may vary, depending on the processor rating of your AS/400 system and the processor speed of the Integrated Netfinity Server.

8.10 Determining the port to Windows NT Server adapter number

As part of the installation and configuration process, Windows NT Server autodetects the LAN adapters and assigns them an adapter number. This number *may not* correspond to the port number assigned by the AS/400 system (Figure 350 on page 302, and Figure 351 on page 303). By disconnecting the LAN cable for one of the ports and using the `PING` command, you can determine which port is assigned to which adapter number.

Table 59. Port number to adapter number mapping

Port number	Adapter number	IP address pinged	Network address
1			
2			
3			
4			

To determine the port number to adapter number relationship, use the following procedure:

1. Unplug *all* the LAN cables from the MAU, hub, or switch that are attached to the Integrated Netfinity Server. This means that only the internal LAN adapter is connected to a network.
2. Plug the LAN cable attached to port 1 (Figure 350 on page 302 and Figure 351 on page 303) into the MAU, hub, or switch for the network assigned to adapter 1.
3. Issue the `PING` command from a Windows NT Server command prompt. Attempt to ping an address that is known to be active, such as a router or server that is in the network assigned to adapter 1. In our example, this would be an address in the 10. network. If a good response is returned, port 1 is mapped to adapter 1. Record this information in Table 59, label the cable as adapter 1, and skip to step 8 of this procedure.
4. Issue the `PING` command from a Windows NT Server command prompt. Attempt to ping an address that is known to be active, such as a router or server that is in the network assigned to adapter 2. In our example, this would be an address in the 10. network. If a good response is returned, port 1 is mapped to adapter 2. Record this information in Table 59, label the cable as adapter 2, and skip to step 8 of this procedure.
5. Unplug the LAN cable attached to port 1 (Figure 350 on page 302, and Figure 351 on page 303) from the current MAU, hub, or switch. Plug the LAN cable attached to port 1 into the MAU, hub, or switch for the network assigned to adapter 2.
6. Issue the `PING` command from a Windows NT Server command prompt. Attempt to ping an address that is known to be active, such as a router or server that is in the network assigned to adapter 1. In our example, this would be an address in the 10. network. If a good response is returned, port 1 is mapped to adapter 1. Record this information in Table 59, label the cable as adapter 1, and skip to step 8 of this procedure.

7. Issue the `PING` command from a Windows NT Server command prompt. Attempt to ping an address that is known to be active, such as a router or server that is in the network assigned to adapter 2. In our example, this would be an address in the 208.222.150.248 network. If a good response is returned, port 1 is mapped to adapter 2. Record this information in Table 59 on page 316, label the cable as adapter 2, and skip to step 8 of this procedure.
8. Unplug the LAN cable attached to port 1 from the MAU, hub, or switch.
9. Plug the LAN cable attached to port 2 (Figure 350 on page 302 and Figure 351 on page 303) into the MAU, hub, or switch for the network assigned to adapter 1.
10. Issue the `PING` command from a Windows NT Server command prompt. Attempt to ping an address that is known to be active, such as a router or server that is in the network assigned to adapter 1. In our example, this would be an address in the 10. network. If a good response is returned, port 2 is mapped to adapter 1. Record this information in Table 59 on page 316, label the cable as adapter 1, and skip to step 16 of this procedure.
11. Issue the `PING` command from a Windows NT Server command prompt. Attempt to ping an address that is known to be active, such as a router or server that is in the network assigned to adapter 2. In our example, this would be an address in the 208.222.150.248 network. If a good response is returned, port 2 is mapped to adapter 2. Record this information in Table 59 on page 316, label the cable as adapter 1, and skip to step 16 of this procedure.
12. Unplug the LAN cable attached to port 2 (Figure 350 on page 302 and Figure 351 on page 303) from the current MAU, hub, or switch. Plug the LAN cable attached to port 2 into the MAU, hub, or switch for the network assigned to adapter 2.
13. Issue the `PING` command from a Windows NT Server command prompt. Attempt to ping an address that is known to be active, such as a router or server that is in the network assigned to adapter 1. In our example, this would be an address in the 10. network. If a good response is returned, port 2 is mapped to adapter 1. Record this information in Table 59 on page 316, label the cable as adapter 1, and skip to step 16 of this procedure.
14. Issue the `PING` command from a Windows NT Server command prompt. Attempt to ping an address that is known to be active, such as a router or server that is in the network assigned to adapter 2. In our example, this would be an address in the 208.222.150.248 network. If a good response is returned, port 2 is mapped to adapter 2. Record this information in Table 59 on page 316, label the cable as adapter 2, and skip to step 16 of this procedure.
15. If you have a third LAN adapter in your Integrated Netfinity Server, unplug the LAN cable attached to port 2 from the MAU, hub, or switch. Repeat steps 9 through 14 using port 3 rather than port 2.
16. Plug the cables into the *correct* MAU, hub, or switch based on the cable labels and the information recorded in Table 59 on page 316. Test the connections by using the `PING` command to ping an address in each network. As a final test of your network connectivity, you should go to another system in each of the networks and ping the IP addresses assigned to Integrated Netfinity Server ports. If this is successful, your adapters are connected correctly and you are ready to proceed with the set-up process.

The results of our testing with this procedure are shown in Table 60.

Table 60. Sample port number to adapter number mapping

Port number	Adapter number	IP address pinged	Network address
1	2	208.222.150.249	208.222.150.248
2	1	10.1.1.1	10.
3 *internal	3	192.168.2.2	192.168.2
4	N/A	N/A	N/A

You are now ready to complete the post-installation task for Windows NT Server.

8.11 Completing the post-installation tasks

Here are some additional tasks that you need to perform to complete the setup. Notice that some of these tasks may not apply to you.

1. Reconnect the LAN adapter.

If you physically disconnected one of your LAN adapters before the installation, reconnect it now. You need to restart the server to make this line active.

2. Verify the display settings.

Verify the display settings for the display attached to the Integrated Netfinity Server. IBM eNetwork Firewall for Windows NT requires a display that is capable of at least 1024 x 768 resolution.

3. Change the CD-ROM drive letter.

We recommend that you use Windows NT Disk Administrator to assign the CD-ROM to drive X:. This stops the CD-ROM drive from changing drive letters every time you link a user storage space to the server.

Complete the following steps to change the CD-ROM drive letter.

- Click **Start->Programs->Administrative Tools (Common)->Disk Administrator**. The Disk Administrator window appears.
- Right-click in the window next to the **CD-ROM** label.
- Click **Assign Drive Letter....** The Assign Drive Letter window appears.
- Select the new drive letter from the drop-down menu.
- Click **OK**.

4. Change the retain server security (QRETSVRSEC) system value.

To propagate AS/400 user profile information across to Windows NT, the AS/400 system value QRETSVRSEC must be set to 1 (retain data).

- On an AS/400 command line, type:
`WRKSYSVAL SYSVAL(QRETSVRSEC)`

Press Enter.

- Enter 2 in the Option column to change the system value.
- Change the system value to 1, and press Enter.

5. Vary on the Windows NT server at IPL with V4R4.

Notice that you can no longer change the Online at IPL parameter in the network server description in Version 4 Release 4 as you could in previous releases. However, you can configure TCP/IP so that the Windows NT Server is automatically varied on when you start TCP/IP.

To setup online with TCP/IP, perform these steps:

- a. Type `CFGTCP` on an AS/400 command line, and press Enter.
- b. Select option **1**, and press Enter.
- c. Type **2** in the Option column next to the interface for the server internal LAN line, and press Enter.
- d. Type `*YES` for the Automatic start parameter, and press Enter.

The network server description for the Windows NT Server automatically varies on when you start TCP/IP.

Make sure that you only have one network server description defined for each Integrated Netfinity Server with the internal LAN interface set to start automatically.

We recommend that you start TCP/IP in your startup program, and do *not* specifically vary on the network server description. In this case, the possibility of the network server timing out while waiting for TCP/IP to start is averted.

6. Vary on the server at IPL for V4R2 and V4R3 only.

This capability is disabled in Version 4 Release 4.

You should not select this option unless you specify the Start TCP/IP (`STRTCP`) command in the AS/400 system startup program. Otherwise, you may find that the network server description does not become active because TCP/IP is not started when the server tries to vary on.

To automatically vary on the server at IPL, follow these steps:

- a. Type `CFGNWS` on an AS/400 command line, and press Enter.
- b. Type the name of the network server description, and press **F9**.
- c. Type `*YES` for the Online at IPL parameter, and press Enter.

Make sure that you only have one network server description defined for each Integrated Netfinity Server with the Online at IPL parameter set to `*YES`.

We recommend that you include the command to vary on the network server description in your AS/400 startup program after the Start TCP/IP (`STRTCP`) command. In this case, you can also insert a Delay Job (`DLYJOB`) command after the `STRTCP` command to make sure that TCP/IP is started before the network server starts to vary on.

7. Remove unused protocols from the communications environment. Follow these steps:

- a. Right-click the **Network Neighborhood**.
- b. Select **Properties**.
- c. Click the **Protocols** tab.
- d. Select an unused protocol (NetBEUI, IPX/SPX and NetBIOS), and then click **Remove**.
- e. Repeat step "d" until all unused protocols are removed.
- f. Click **OK**. IPL as needed.

8. Install The Microsoft DNS Server using the selective installation of Windows NT Server 4.0.

9. Refer to Section 4.5 of *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT*, SG24-5209, for more recommendations on tightening the security in Windows NT Server 4.0.

10. Install the Windows NT Service Pack.

Before you put a Windows NT Server into regular operation, you *must* apply any required Windows NT Service Packs.

Note: Windows NT Server 4.0, running on the Integrated Netfinity Server, requires Windows NT Server Service Pack 3 or later to be installed. IBM eNetwork Firewall for Windows NT requires Windows NT Server Service Pack 4 or later to be installed.

For the latest information on supported Windows NT Service Packs, visit the web site: <http://www.as400.ibm.com/nt>

Select **Service Information** on the left side of the display, and then **Service Packs** on the right side of the display

11. Set the Windows NT Server startup time to a small value.

Perform the following steps to change the startup time:

- a. Right-click **My Computer->properties**.
- b. Select the **Startup/Shutdown** tab.
- c. Change the value in the **Show list for** box to 5 seconds.
- d. Click **OK**.

12. Reset the performance adjustment (QPRFADJ) system value.

If you set the QPFRADJ system value to 2 or 3 before the installation, you may now want to set it back to its previous value. It is preferable to wait a day or so to ensure that the AS/400 system has had time to make adjustments to the machine pool. Use the Work with System Values (`WRKSYSVAL`) command to reset it, if required.

13. Back up Windows NT system drives.

We recommend that you back up the Windows NT C:, D:, and E: drives at this time. This makes recovery easier if the Windows NT Server becomes corrupt because you can simply restore a working copy of the failed drive. See *AS/400 - Implementing Windows NT on the Integrated Netfinity Server*, SG24-2164, for information about backing up these drives.

You have now completed the installation of Windows NT on the Integrated Netfinity Server. You are now ready to install IBM eNetwork Firewall for Windows NT product.

Appendix A. Implementing other firewall functions

This appendix shows how to implement additional functions that are included in the Firewall for AS/400 product. These functions are implemented using a package file and do not have a GUI configuration tool available. These functions are available but *not* supported.

Note: Use these functions at your own risk.

A.1 Creating and using a package file

Each *base type of network server description has a parameter that can be used to specify a configuration file and library. The command keyword for this parameter is CFGFILE. This is used to point to a source physical file that contains package files that can be used to update the firewall configuration. This library should be secure to prevent unauthorized changes from being made to the firewall.

To configure additional functions, you must perform these steps:

1. Create a library to contain the package file.
2. Create the source physical file to contain the package members.
3. Add members to the package file to make the configuration changes.
4. Change the network server (NWS) description to use the package file.
5. Vary off and vary on the NWS.

To create the library for the package file, use the AS/400 Create Library (CRTLIB) command. We named our library FIREUPDT.

```
CRTLIB LIB(FIREUPDT) TEXT('Add additional function for firewall')
```

To create the source physical file for the package file, use the AS/400 command CRTSRCPF. The source physical file must have a length of 92. This is the default length on the command. We named our file UPDTSRC.

```
CRTSRCPF FILE(FIREUPDT/UPDTSRC) TEXT('Source file for the package file')
```

We use the SEU editor under PDM to add the source members as needed. In most cases, the members should remain in the package file at all times because many of the firewall files are built fresh when the NWS is varied on. Refer to the other sections in the appendix for the contents of the members in the package file.

To change the network server description, use the AS/400 Change Network Server Description (CHGNWSD) command. Our NWS is named FW1MAIL. To add the package file to the NWS configuration, we used the following command:

```
CHGNWSD NWS(FW1MAIL) CFGFILE(FIREUPDT/UPDTSRC)
```

Use your normal method of stopping and starting the firewall application and network server configuration.

A.2 IP address alias on the secure LAN

This is an example of how to add a second IP address, 10.1.1.8, to the firewall secure port. This only works on V4R3M0 or greater. Prior releases with older TCP/IP do not support aliases. Check the filter rules for the existing secure IP address. You may need to duplicate those rules for the new IP address. If your secure LAN is composed of multiple subnets with routers using the new IP addresses, the firewall network server description must be changed to add routes to those addresses through the new interface alias.

Before you code the package file, you must determine the name of the secure port on the firewall. It may be named LAN0, LAN1, or LAN2. To determine the correct value, use the AS/400 command:

```
SBMNWSCMD CMD('type e:\mptn\bin\setup.cmd') SERVER(FW1MAIL) SVRTYPE(*BASE)
```

Display your job log and look at the contents of the setup.cmd file (Figure 360).

```
route -f
arp -f
rem ipgate off
ifconfig lan0 10.1.1.7 netmask 255.255.255.0 metric 0 mtu 1500
ifconfig lan1 208.222.150.250 netmask 255.255.255.248 metric 0 mtu 1500
ifconfig lan2 192.168.2.2 netmask 255.255.255.0 metric 0 mtu 8000
route add net      default          208.222.150.249 -hopcount 64 netmask
0.0.0.0
route add net      10                10.1.1.1         -hopcount 64 netmask
255.0.0.0
Command submitted to server FW1MAIL.
```

Figure 360. Contents of the e:\mptn\bin\setup.cmd file

Find the address of the secure port of your firewall. In our case, this is 10.1.1.7. The value just before the address is the name of the LAN adapter. In this example, it is LAN0. We use this information to build the package file shown in Figure 361 on page 323.

```

*****
* DEFAULTS
*****
SETDEFAULTS
  TARGETDIR = 'E:\MPTN\BIN', TARGETFILE = 'SETUP.CMD',
  ADDWHEN   = 'ALWAYS', DELETEWHEN = 'NEVER'
*=====
* Add interface alias
*=====
ADDCONFIG
  ADDSTR = 'IFCONFIG LANO 10.1.1.8 NETMASK 255.255.255.0 ALIAS MTU 1500',
  UNIQUE = 'YES'
*=====
SETDEFAULTS
  TARGETDIR = 'E:\FIREWALL\ETC', TARGETFILE = 'FWSECAD.CNF',
  ADDWHEN   = 'ALWAYS', DELETEWHEN = 'NEVER'
*=====
* Define new alias as a secure interface
*=====
ADDCONFIG ADDSTR = '10.1.1.8', UNIQUE = 'YES'

```

Figure 361. Package file to add an additional IP address to the secure port

To remove this change, you only need to remove the line added to the FWSECAD.CNF file. The SETUP.CMD is built at each vary off and vary on of the NWS. The package file to do this is shown in Figure 362.

```

*=====
SETDEFAULTS
  TARGETDIR = 'E:\FIREWALL\ETC', TARGETFILE = 'FWSECAD.CNF',
  ADDWHEN   = 'NEVER', DELETEWHEN = 'ALWAYS'
*=====
* Remove interface from secure adapters file
*=====
ADDCONFIG ADDSTR = '10.1.1.8', UNIQUE = 'YES'

```

Figure 362. Package file to remove an additional IP address from the secure port

A.3 IP address alias on the non-secure LAN

This is an example of how to add a second IP address, 208.222.150.251, to the firewall non-secure port. This only works on V4R3M0 or greater. Prior releases with older TCP/IP do not support aliases. Check the filter rules for the existing secure IP address. You may need to duplicate those rules for the new IP address.

You may want to add additional addresses on the non-secure port so that static Network Address Translation (NAT) addresses will be ARPed by the firewall and the ISP router will pass these packets to the firewall.

This technique is similar to the technique in A.2, “IP address alias on the secure LAN” on page 322. The difference is that for the non-secure interface, you *do not* include the ADDCONFIG for the FWSECAD.CNF file, since this IP address is not a secure interface. Again, filter rules should be reviewed and duplicated where appropriate.

Before you code the package file, you must determine the name of the secure port on the firewall. It may be named LAN0, LAN1, or LAN2. To determine the correct value, use the AS/400 command:

```
SBMNWSCMD CMD('type e:\mptn\bin\setup.cmd') SERVER(FW1MAIL) SVRTYPE(*BASE)
```

Display your job log and look at the contents of the setup.cmd file (Figure 360 on page 322).

Find the address of the non-secure port of your firewall. In our case, this is 208.222.150.250. The value just before the address is the name of the LAN adapter. In this example, it is LAN1. We use this information to build the package file in Figure 363.

```
*****
* DEFAULTS
*****
SETDEFAULTS
  TARGETDIR = 'E:\MPIN\BIN', TARGETFILE = 'SETUP.CMD',
  ADDWHEN   = 'ALWAYS', DELETEWHEN = 'NEVER'
*=====
* Add interface alias
*=====
ADDCONFIG
  ADDSTR = 'IFCONFIG LAN1 208.222.150.251 NETMASK 255.255.255.248 ALIAS MTU 1500',
  UNIQUE = 'YES'
```

Figure 363. Package file to add an additional IP address to the non-secure port

To remove this change, delete the member from the package file or remove the `addconfig` for the address you want removed. The `SETUP.CMD` is built at each vary off and vary on of the NWS.

A.4 Preventing spam mail from reaching secure clients

This section explains how to block incoming mail using three different criteria. The selection criteria are source mail domain, sender name and domain, or source IP address.

A.4.1 Blocking spam by domain name

This is an example of how to create a list of domains from which the firewall will reject mail. The file `e:\firewall\etc\spamlist`, must exist on the NWS for this package file to work. Issue the following command to create the file. This only needs to be done once for the existence of the NWS:

```
SBMNWSCMD CMD('echo > e:\firewall\etc\spamlist') SERVER(<nwsd_name>)
SVRTYPE(*BASE)
```

Use a package file to put domain names into the file you created. An example of a file to block mail from specific domains is shown in Figure 364 on page 325. You may add as many domains as you need to block. Each domain must be listed in a separate `ADDCONFIG` directive. In this example, we block two domains.

```

*****
* DEFAULTS
*****
SETDEFAULTS
  TARGETDIR = 'E:\FIREWALL\ETC', TARGETFILE = 'SPAMLIST',
  ADDWHEN   = 'ALWAYS', DELETEWHEN = 'NEVER'
*=====
* Clear list and add the following members
*=====
CLEARCONFIG TARGETDIR = 'E:\FIREWALL\ETC', TARGETFILE = 'SPAMLIST'
*
ADDCONFIG ADDSTR = 'spamcity.com', UNIQUE = 'YES'
ADDCONFIG ADDSTR = 'otherspam.com', UNIQUE = 'YES'

```

Figure 364. Package file to block e-mail based on a domain name

To remove domains from the spam list, delete the domain entry from the source member. The `CLEARCONFIG` directive clears the file at each vary off or vary on of the NWS. Only those entries in the package file will be added to the file.

A.4.2 Blocking spam by sender name and domain

This is an example of how to create a list of fully-qualified hosts from which the firewall will reject mail. The file `e:\firewall\etc\spamname` must exist on the NWS for this package file to work. Issue the following command to create the file. This only needs to be done once for the existence of the NWS:

```

SEMNWSCMD CMD('echo > e:\firewall\etc\spamname') SERVER(<nwsd_name>)
SVRTYPE(*BASE)

```

Use a package file to put fully-qualified host names into the file you created. An example of a file to block mail from specific fully-qualified host names is shown in Figure 365. You may add as many names as you need to block. Each name must be listed in a separate `ADDCONFIG` directive. In this example, we block two domains.

```

*****
* DEFAULTS
*****
SETDEFAULTS
  TARGETDIR = 'E:\FIREWALL\ETC', TARGETFILE = 'SPAMNAME',
  ADDWHEN   = 'ALWAYS', DELETEWHEN = 'NEVER'
*=====
* Clear list and add the following members
*=====
CLEARCONFIG TARGETDIR = 'E:\FIREWALL\ETC', TARGETFILE = 'SPAMNAME'
*
ADDCONFIG ADDSTR = 'spammer@spamming.com', UNIQUE = 'YES'
ADDCONFIG ADDSTR = 'spammer2@otherspam.com', UNIQUE = 'YES'

```

Figure 365. Package file to block e-mail based on a fully-qualified name

To remove names from the spam list, delete the name entry from the source member. The `CLEARCONFIG` directive clears the file at each vary off or vary on of the NWS. Only those entries in the package file are added to the file.

A.4.3 Blocking spam by source IP address

This is an example of how to create a list of IP addresses from which the firewall will reject mail. The file `e:\firewall\etc\deniedip` must exist on the NWS for this package file to work. Issue the following command to create the file. This only needs to be done once for the existence of the NWS:

```
SEMNWSCMD CMD('echo > e:\firewall\etc\deniedip') SERVER(<nwsd_name>)
SVRTYPE (*BASE)
```

Use a package file to put IP addresses into the file you created. An example of a file to block mail from specific IP addresses is shown in Figure 366. You may add as many IP addresses as you need to block. Each IP address must be listed in a separate `ADDCONFIG` directive. In this example, we block two IP addresses.

```
*****
* DEFAULTS
*****
SETDEFAULTS
  TARGETDIR = 'E:\FIREWALL\ETC', TARGETFILE = 'DENIEDIP',
  ADDWHEN   = 'ALWAYS', DELETEWHEN = 'NEVER'
*=====
* Clear list and add the following members
*=====
CLEARCONFIG TARGETDIR = 'E:\FIREWALL\ETC', TARGETFILE = 'DENIEDIP'
*
ADDCONFIG ADDSTR = '208.222.27.1', UNIQUE = 'YES'
ADDCONFIG ADDSTR = '208.222.27.2', UNIQUE = 'YES'
```

Figure 366. Package file to block e-mail based on fully-qualified name

To remove the IP addresses from the spam list, delete the IP address entry from the source member. The `CLEARCONFIG` directive clears the file at each vary off or vary on of the NWS. Only those entries in the package file are added to the file.

A.5 Nesting firewalls in a network

Changes are needed to the DNS and the proxy server of the firewall when the firewall is behind another firewall. If these changes are not made, the firewall will not work correctly.

A.5.1 Adding forwarders to the firewall DNS configuration

Two directives that point to the external DNS are inserted into the DNS boot file (`NAMED.BT`). This example has the AS/400 firewall DNS forwarding all requests for which it does not have answers to the DNS server at IP address 128.63.2.53, presumably the outer firewall's DNS (Figure 367).

```

*=====
* Defaults
*=====
SETDEFAULTS
  TARGETDIR   = 'E:\FIREWALL\ETC\NAMEDB', TARGETFILE = 'NAMED.BT',
  ADDWHEN     = 'ALWAYS', DELETEWHEN = 'NEVER'
*=====
* Boot file directives
*=====
ADDCONFIG ADDSTR = 'forwarders 128.63.2.53', UNIQUE = 'YES'
ADDCONFIG ADDSTR = 'slave', UNIQUE = 'YES'

```

Figure 367. Package file to add forwards to the firewall DNS

To remove this change, you only need to remove the lines added to the NAMED.BT file. This is done by changing the ADDWHEN and DELETEWHEN values in the package file. The package file to do this is shown in Figure 368.

```

*=====
* Defaults
*=====
SETDEFAULTS
  TARGETDIR   = 'E:\FIREWALL\ETC\NAMEDB', TARGETFILE = 'NAMED.BT',
  ADDWHEN     = 'NEVER', DELETEWHEN = 'ALWAYS'
*=====
* Remove forwarders and slave directives
*=====
ADDCONFIG ADDSTR = 'forwarders 128.63.2.53', UNIQUE = 'YES'
ADDCONFIG ADDSTR = 'slave', UNIQUE = 'YES'

```

Figure 368. Package file to remove forwards from the firewall DNS

A.5.2 Chaining the HTTP proxy to another server

To allow the proxy server to chain to another proxy server, create another member in the source physical file. This adds a directive to the HTTPD.CNF file in the AS/400 firewall configuration. Substitute your outer proxy name or IP address for the single occurrence of the string `outer.proxy.server` in the package file shown in Figure 369.

```

*=====
* Defaults
*=====
SETDEFAULTS
  TARGETDIR   = 'E:\FIREWALL\ETC', TARGETFILE = 'HTTPD.CNF',
  ADDWHEN     = 'ALWAYS', DELETEWHEN = 'NEVER'
*=====
* HTTP proxy file directives
*=====
ADDCONFIG ADDSTR = 'http_proxy http://outer.proxy.server/',
  UNIQUE = 'YES', FILESEARCHPOS='AFTER',
  FILESEARCHSTR='# http_proxy   outer_http_proxy.ibm.com'

```

Figure 369. Package file to add HTTP proxy chaining to the HTTP proxy

To remove this change, you only need to remove the line that was added to the HTTPD.CNF file. This is done by changing the ADDWHEN and DELETEWHEN values in the package file. The package file to do this is shown in Figure 370.

```
*=====
* Defaults
*=====
SETDEFAULTS
  TARGETDIR = 'E:\FIREWALL\ETC', TARGETFILE = 'HTTPD.CNF',
  ADDWHEN   = 'NEVER', DELETEWHEN = 'ALWAYS'
*=====
* HTTP proxy file directives
*=====
ADDCONFIG ADDSTR = 'http_proxy http://outer.proxy.server/',
  UNIQUE = 'YES'
```

Figure 370. Package file to remove HTTP proxy chaining from the HTTP proxy

Appendix B. Using virtual IP addresses

This appendix explains the use of virtual IP addresses. It provides information about how to configure virtual IP addresses on the AS/400 system.

B.1 What is a virtual IP address?

A virtual IP address, or circuitless connection, is an IP interface that is defined on the system without being associated with a physical hardware adapter. These addresses can always be active on the system. These addresses can be used as the “system” IP address. These addresses are always reached indirectly through a real TCP/IP interface and do not respond to ARP requests. For other systems to reach the virtual IP address, they must have a route defined to reach the address. The AS/400 system accepts IP packets on any interface and processes the packet if the IP address is defined on any interface on the system. This provides a way to assign one or more addresses to the system without needing to bind the address to a physical interface. This can be used when you want to run multiple occurrences of a Domino Web server bound to different addresses, or other services, such as HTTP servers, that need to bind to default ports.

Virtual IP address support was added in V4R3 of the OS/400 operating system. This feature can be used when consolidating multiple systems into one large system.

B.2 Configuring virtual IP addresses

The addresses that you set up as virtual IP addresses cannot be a part of any real network segment in your network. Choose a network address range that is unused in your environment. Figure 371 shows a sample network that we discuss in this section.

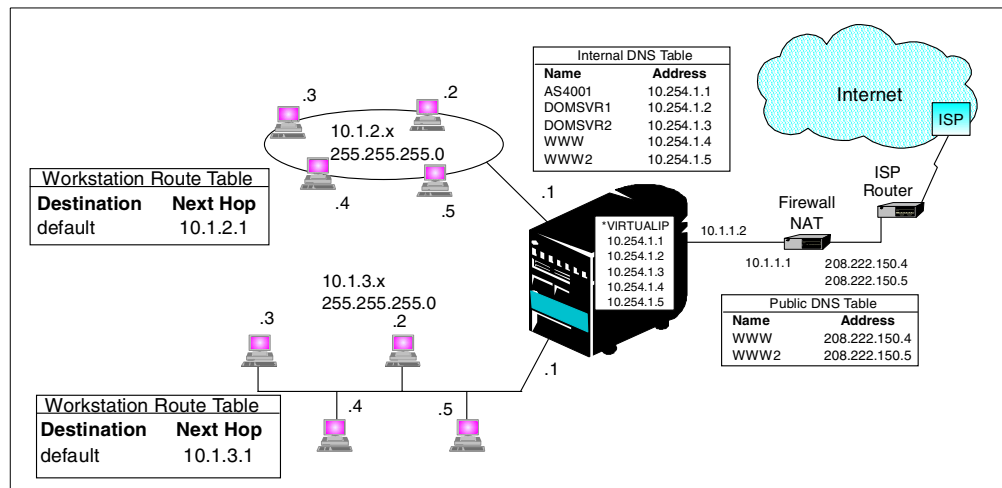


Figure 371. Sample network using virtual IP addresses

In this example, the workstations all point to the AS/400 system as their next hop gateway. The firewall uses Network Address Translation (NAT) to change the public address 208.222.150.4 to 10.254.1.4, and the public address

208.222.150.5 to 10.254.1.5. The firewall has a route entry that directs all "10." traffic to AS/400 interface 10.1.1.2. When a packet arrives at the AS/400 system, it goes through the packet processing. If the destination address matches any address defined on the system (including virtual IP addresses), the system processes the packet.

B.2.1 Task summary

To set up the virtual IP address, we perform the following steps:

1. Select a network address to use as virtual IP addresses.
2. Define the Virtual IP addresses on the system.
3. Add the route entries to any systems that need to access the system using the virtual IP addresses.
4. Add the system names to the DNS.
5. Start the interfaces that have the virtual IP address defined.
6. Test the connectivity.

B.2.2 Selecting a network address to use as virtual IP addresses

The first step in configuring virtual IP addresses is to select an address range to use as virtual IP addresses. This subnet of addresses must not be used anywhere else in the network. The address range cannot be a part of an existing subnet. The addresses in this range cannot respond to an ARP request. In our example, we selected a range that should be well out of the way of the rest of the network. Our sample network shown in Figure 371 on page 329 uses the 10. network for private addresses. After checking our network documentation, we determined that the 10.255.1 subnet was not in use. Because it is such a high address range, it should be out of the way of future growth.

B.2.3 Defining the virtual IP addresses on the system

Once you determine the address range that you are going to use, you need to create the TCP/IP interfaces on the system that will use the addresses. To add the virtual IP addresses on the system, you can either use the AS/400 command `ADDTCPIFC`, or you may use Operations Navigator. To add the first interface, we entered the command:

```
ADDTCPIFC INTNETADR('10.254.1.1') LIND(*VIRTUALIP) SUBNETMASK(*HOST)
MTU(16388)
```

We specified a subnet mask of `*HOST` so that we may use other addresses in the network range as virtual addresses on other systems. You must also specify an MTU size because there is not a physical line description for the command to use to determine the frame size. The MTU size does not impact performance because the interface is virtual. The route and physical interface taken out of the system determines the real MTU size.

To add the second interface, we used Operations Navigator. Refer to Figure 372 on page 331 as you perform the following procedure to start the add process:

1. Double-click the system name **AS07** (A).
2. Double-click **Network** (B).
3. Click **Protocols** (C).
4. In the right window, right-click **TCP/IP**, and select **New Interface->Circuitless** (C). An information screen displays (not shown). Click **Next**. The display shown in Figure 373 on page 331 appears without the values filled in.

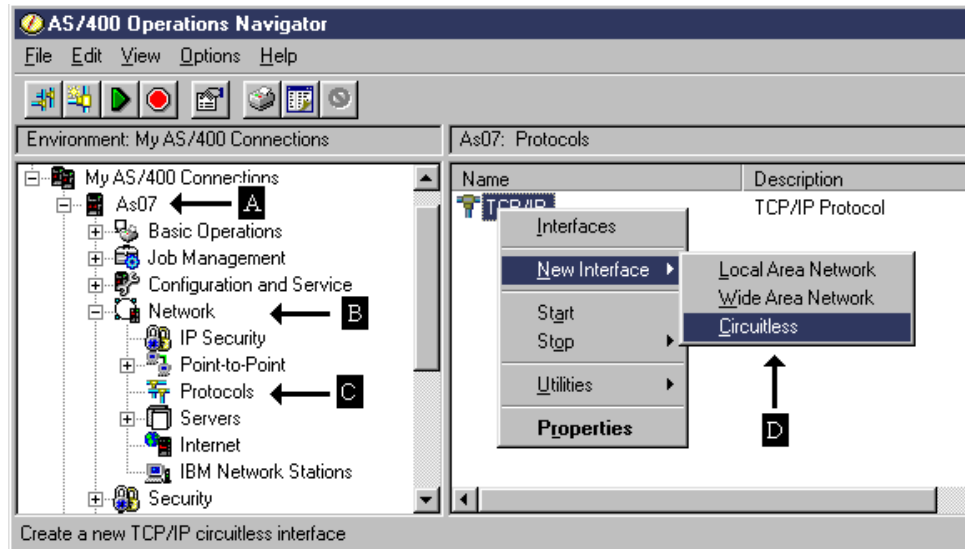


Figure 372. Adding a virtual IP address

- Enter the virtual IP address, a name for the interface (used in Operations Navigator only), and the subnet mask value as shown in Figure 373. Click **Next**. The Start TCP/IP Interface window (not shown) is displayed. Select your start values for the interface, and click **Next**. The New TCP/IP Interface Summary window appears (Figure 374).

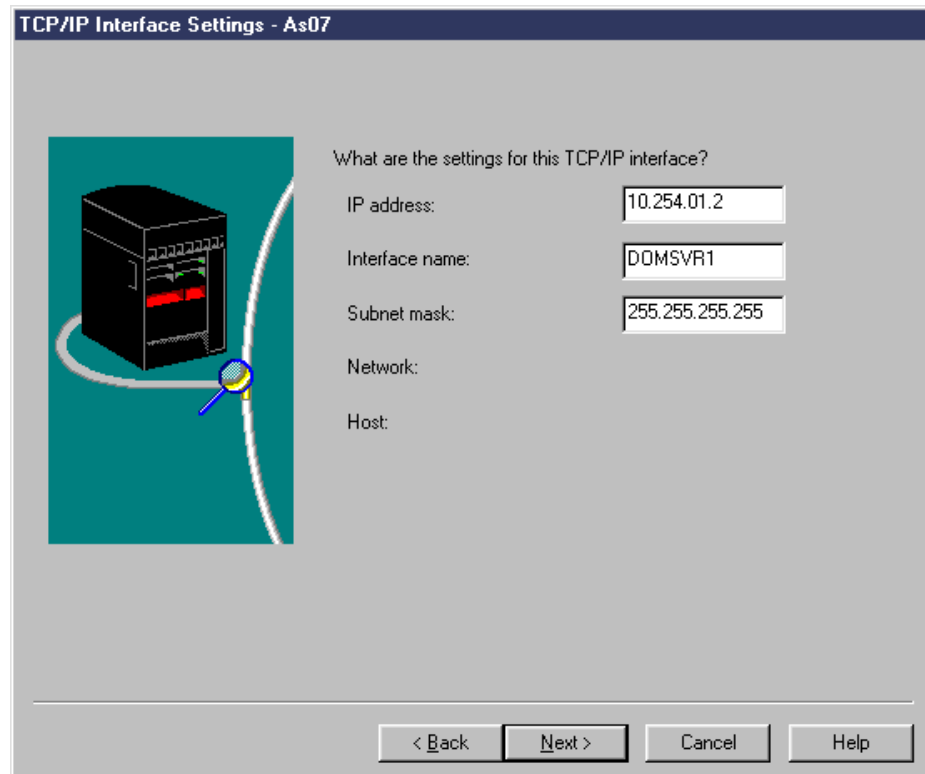


Figure 373. Specifying the IP address information

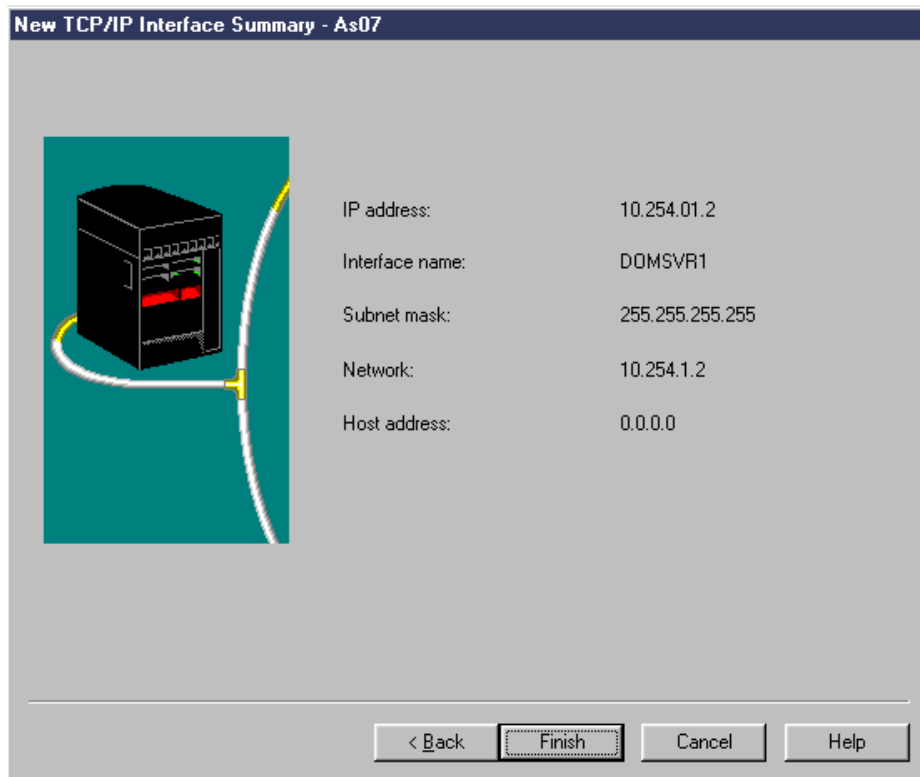


Figure 374. New TCP/IP Interface Summary display

6. Verify that the values shown are correct. If they are correct, click **Finish**. If they are incorrect, use the **Back** button to backup and correct the error. When you click Finish, you are given an opportunity to test the interface. Click **Test now**. After the test, click **OK** to exit the add function.

The virtual IP address is now added. Repeat the steps as needed to add the remaining IP addresses. Figure 375 on page 333 shows the Work with TCP/IP Interfaces (CFGTCP option 1) display after all the adds are complete for the interfaces.

```

Work with TCP/IP Interfaces
System: AS07

Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  9=Start  10=End

  Internet      Subnet      Line      Line
Opt Address      Mask        Description Type
---
  10.1.1.2      255.255.255.0  ETHLINE1  *ELAN
  10.1.2.1      255.255.255.0  TRNLINE   *TRLAN
  10.1.3.1      255.255.255.0  ETHLINE2  *ELAN
  10.254.1.1    255.255.255.255 *VIRTUALIP *NONE
  10.254.1.2    255.255.255.255 *VIRTUALIP *NONE
  10.254.1.3    255.255.255.255 *VIRTUALIP *NONE
  10.254.1.4    255.255.255.255 *VIRTUALIP *NONE
  10.254.1.5    255.255.255.255 *VIRTUALIP *NONE

More...

F3=Exit      F5=Refresh  F6=Print list  F11=Display interface status
F12=Cancel   F17=Top     F18=Bottom

```

Figure 375. TCP/IP interfaces with all addresses added

B.2.4 Adding the route entries

Go to each system that needs to access the virtual IP addresses and add the correct routing entry. For most of the systems, this will consist of a default route with a next hop that points to the real AS/400 interface. In some cases, a more specific route entry may be needed.

This information is added to a windows workstation by specifying a gateway entry in the TCP/IP properties of the network configuration. The information can also be passed in the DHCP configuration information that is passed to a workstation that is using DHCP to determine its TCP/IP address. Using DHCP is the recommended approach because it puts all the TCP/IP configuration for the workstations in a central location.

You need to make the appropriate route entries in any routers that need to point to these virtual IP addresses. You may distribute the route to the virtual IP addresses to other systems and routers in the network using RIPV2. This is done by starting the Router Daemon on the AS/400 system using the command:

```
STRTCPSVR SERVER(*ROUTED)
```

B.2.5 Adding the system names to the DNS

Add the system names to the DNS server in the internal network. Refer to 3.2, “Configuring the AS/400 DNS” on page 21, for an example of the DNS configuration. For detailed instructions, refer to *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147.

B.2.6 Starting the interfaces

If you did not choose to start the TCP/IP interfaces as you created them, you need to start them now. To start the interfaces, go to the Work with TCP/IP Interfaces (CFGTCP option 1) as shown in Figure 375 on page 333. Enter a 9 in the

option area in front of each interface you want to start. Press Enter. The interfaces should start.

B.2.7 Testing the connectivity

After all the interfaces are started, test the connectivity to ensure that everything is working. The easiest way to do this is by using the `PING` command.

Go to a workstation and try to ping one of the virtual IP addresses. You should receive a successful completion message. If you do not, check the route information in the workstation and any routers that may be in the network. If the ping works using an address, try it using the name you assigned to the virtual IP address. If the ping by address worked, but the ping by name fails, you have a DNS problem.

Repeat the ping test for each virtual address you defined. Perform a ping using the address first and then a ping using the name of each interface.

After all the ping tests in the internal network work, go to the external network and try accessing a server. A ping test may not work from the outside because most firewalls block the `PING` command.

B.3 Virtual IP addresses and e-mail

Virtual IP addresses work well in situations where you need unique TCP/IP addresses to bind to applications. One example of this is when you set up multiple Domino servers on the same system. The recommendation is to define a new address for each new server. While you can add multiple IP addresses to a physical interface, this can lead to problems at times when a request comes in with one address but is responded to with another address.

Another problem can result. If the physical interface is varied off, the IP addresses associated with the interface are not available. With a virtual IP address, the interface can be active as long as the system is active. This may result in higher availability.

Appendix C. DNS concepts

This appendix presents some basic concepts about the Domain Name Server (DNS) system. It contains an excerpt from the redbook *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147.

C.1 IBM eNetwork Firewall for Windows NT DNS implementation

IBM eNetwork Firewall for Windows NT uses the Microsoft DNS server in a cache-only mode. The Microsoft DNS server is part of the Windows NT server product.

The overall naming service framework for the firewall requires two additional DNS servers: a name server in the secure network (AS/400 DNS in our scenarios) and a name server in the public network. The secure name server maintains a complete database of all internal systems and domains. The public name server only contains information about public servers (Web server, for example).

C.2 Overview

The Domain Name System is a distributed database. This allows local control of the segments of the entire database, and data in each segment is also available across the entire network through a client/server scheme.

The structure of the DNS database is similar to the structure of a file system. The entire database or file system is pictured as an inverted tree with the root at the top. Each node in the tree represents a partition of the database. Each domain or directory can be further divided into partitions, called *subdomains* (such as the file system's subdirectories).

The domain name space is *tree* structured. The top-level domains divided the Internet domain name space organizationally. Examples of top-level domains are:

- **com**: Commercial organizations, such as IBM (*ibm.com*), CNN (*cnn.com*), and mycompany (*mycompany.com*). *ibm* is a subdomain of the top-level domain *com*.
- **edu**: Educational organizations, such as University of Minnesota (*umn.edu*) and New York University (*nyu.edu*).
- **gov**: Government organizations, such as the Federal Bureau of Investigation (*fbi.gov*) and the National Science Foundation (*nsf.gov*).

The tree is limited to 127 levels. This is a limit on subdomains, although there is no limit on the number of branches at each node.

Each node in the tree is labeled with a name (Figure 376 on page 336). The root has a null label (" "). The full domain name of any node in the tree is the sequence of names on the path from the node up to the root with a dot between node names. For example, in Figure 376 on page 336, if you follow the arrows from the bottom label to the top, from the host: *www* to the root label, you can form the full domain name for that host (*www.as400.ibm.com*).

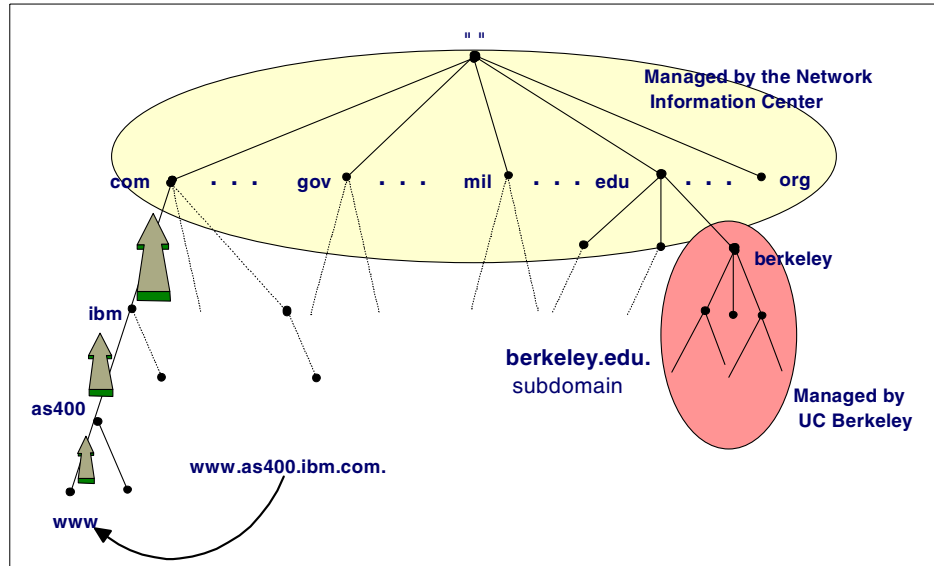


Figure 376. DNS name space

In a DNS, each domain can be administered by a different organization. Each organization can then break its domains into a number of subdomains and dole out the responsibility for those domains to other organizations. This is because DNS uses a distributed database where you can manage your own domain (*company.com*), or parts of the name space (subdomains) can be delegated to other servers (*department.company.com*).

The DNS servers responsible for the top-level Internet domains, such as *com*, are also called *Internet root servers* that manage information about the top-level domains. For example, the Internet's Network Information Center runs the *edu* domain, but assigns U.C. Berkeley authority over the *berkeley.edu* subdomain.

Domains can contain both hosts and other domains (their subdomains). For example, the *ibm.com* domain contains hosts such as *www.ibm.com*, but it also contains subdomains such as *as400.ibm.com*.

Domain names are used as indexes into the DNS database. Each host on a network has a domain name with a DNS server that points to information about the host. This information may include an IP address, information about mail routing, and so on.

Why all this complicated structure? It solves the problems that a host table has. For example, making names hierarchical eliminates the problem of name collisions. Domains are given unique domain names, so organizations are free to choose names within their domains. Whatever name they choose, it does not conflict with other domain names, since it has its own unique domain name.

For example, we can have several hosts named *www*, such as *www.ibm.com* and *www.yahoo.com*, because they are in different domains managed by different organizations. See Figure 377 on page 337.

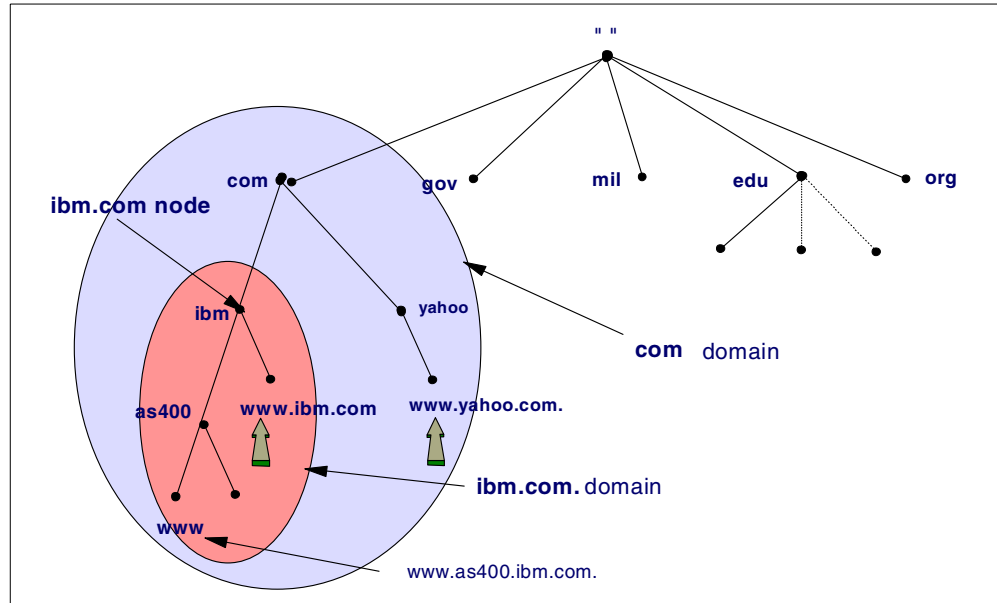


Figure 377. Hosts with the same names in different domains

We can have a host in the same domain that also has the same host name, such as *www.ibm.com* and *www.as400.ibm.com*, because they belong to different subdomains.

C.3 Domain versus zone of authority

The concept of domains versus zones of authority can be confusing. We try to explain it in this section.

One of the goals of the design of the Domain Name System is decentralization. This is achieved through *delegation*. The central DNS administrator in your company administering the company's domain can divide it into subdomains. Each subdomain can be delegated to other administrators. This means that the administrator delegated to becomes responsible for maintaining the subdomain.

A *domain* is a subset or subtree of the name space tree. A *subdomain* is a subset of the domain. Figure 378 on page 339 shows the domain *mycompany.com* as a subset of the *.com* name space. Under *mycompany.com*, there are other subdomains such as *endicott.mycompany.com*, *rochester.mycompany.com*, and *otherdomain.mycompany.com*.

Name Servers are programs running on a system, such as the AS/400 system, with DNS support. In Figure 378 on page 339, *as1.mycompany.com*, *rst.rochester.mycompany.com*, and *otherhost.otherdomain.mycompany.com* are hosts running name server programs. They are called Domain Name System (DNS) servers or simply name servers.

Name servers have information about some part of the domain name space called a *zone* or *zone of authority*. Both domains and zones are subsets of the domain name space. A zone contains host information and data that the domain contains excluding the information that is delegated somewhere else. If a

subdomain of a domain is not delegated, the zone contains host information and data for the subdomain.

Name servers have complete host information and data for a specific zone. Name servers are said to be *authoritative* for the zone for which they have this complete host information and data.

Refer to Figure 378 on page 339. The *mycompany.com* domain is divided into the subdomains: *endicott.mycompany.com*, *rochester.mycompany.com*, and *otherdomain.mycompany.com*. The zone *mycompany.com* contains the hosts: *as1.mycompany.com*, *as2.mycompany.com*, *as5.mycompany.com*, and *NTserver1.mycompany.com*.

It also contains the host information and data in the subdomain *endicott.mycompany.com*: *host1.endicott.mycompany.com* and *host2.endicott.mycompany.com*. The subdomain *endicott.mycompany.com* has not been delegated, and its host information and data remain in the *mycompany.com* zone. The administration of the *endicott.mycompany.com* is the responsibility of the *mycompany.com* administrator. *AS1.mycompany.com* is the name server that has complete host information and data for the *mycompany.com* zone of authority.

The zone *mycompany.com* does *not* contain information in the subdomains that have been delegated.

rochester.mycompany.com is a subdomain of *mycompany.com* and its administration has been delegated. The zone *rochester.mycompany.com* includes host information and data in the subdomain *rochester.mycompany.com*: *rst.rochester.mycompany.com*, *host1.rochester.mycompany.com*, and *host2.rochester.mycompany.com*. *rst.rochester.mycompany.com* is the DNS server that has complete host information and data for the *rochester.mycompany.com* zone.

otherdomain.mycompany.com is a subdomain of *mycompany.com* and its administration has been delegated. The zone *otherdomain.mycompany.com* includes host information and data in the subdomain *otherdomain.mycompany.com*: *otherhost.otherdomain.mycompany.com*, *otherprinter.otherdomain.mycompany.com*, and *otherserver.otherdomain.mycompany.com*. *otherhost.otherdomain.mycompany.com* is the DNS server that has complete host information and data for the *otherdomain.mycompany.com* zone.

AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support, SG24-5147, discusses a scenario in which a subdomain is delegated to another DNS server.

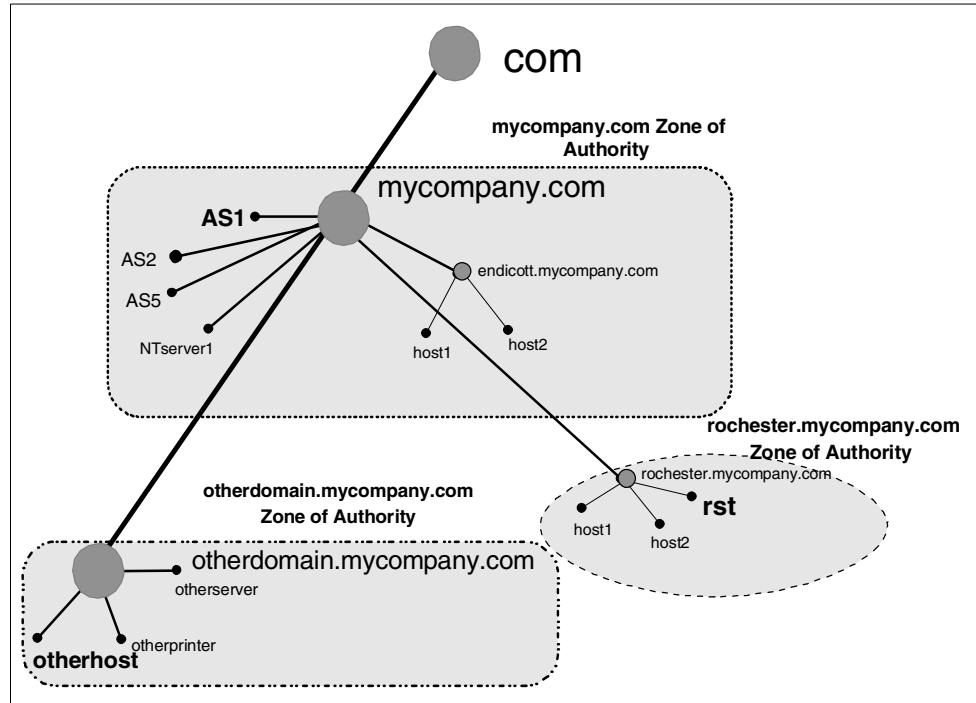


Figure 378. Domain, subdomain, delegation, and zone of authority

C.4 Name resolution

Programs called name servers comprise the server half of the DNS client/server mechanism. Name servers contain information about some segment of the database and make it available to clients, called *resolvers*.

The Domain Name System has two major components:

- **Name servers** are programs that hold information about the domain name space. A name server may cache information about any part of the domain tree but, in general, a particular name server has complete information about a subset of the domain space and pointers to other name servers that can be used to lead to information from any part of the domain tree. The part of the domain space for which the name server has complete information is called a *zone*. It is said that the name server is *authoritative* for that zone. Name servers can be authoritative for multiple zones.
- **Resolvers** are programs that extract information from name servers in response to client requests. Resolvers must be able to access at least one name server and use that name server's information to answer a query. A resolver is typically a system routine that is directly accessible to user programs. No protocol is necessary between the resolver and the user program.

Mapping names to addresses, a process called *domain name resolution*, is provided by independent, cooperating systems called *servers*. A name server is a server program that answers requests from clients called a *name resolver*.

Each name resolver is configured with a name server to use (and possibly a list of alternatives to contact if the primary is unavailable).

Figure 379 schematically shows how a program uses a name resolver to convert a host name to an IP address on the Internet. A user provides a host name, and the user program uses a library routine, called a resolver, to communicate with a name server that resolves the host name to an IP address and returns it to the resolver, which returns it to the main program. The name server may obtain the answer from its name cache (if it has tried to resolve the name before), its own database, or another name server.

In Figure 379, the resolver sends a query for *www.as400.ibm.com* to its DNS server (labeled *primary name server* in the figure). If the query is for information out of the name server's zone of authority (it does not know the answer), the name server sends another query to the Internet root name server, which responds: I don't know but query this next DNS server (the *com* DNS server). Then, the query is iterated to various DNS servers down the "com" branch of the Internet DNS name space until the DNS server is found that is authoritative for (is responsible for) the *as400.ibm.com* domain. This last DNS server has the answer and sends the response back to the original DNS server for which the resolver asked, which passes the response back to the resolver.

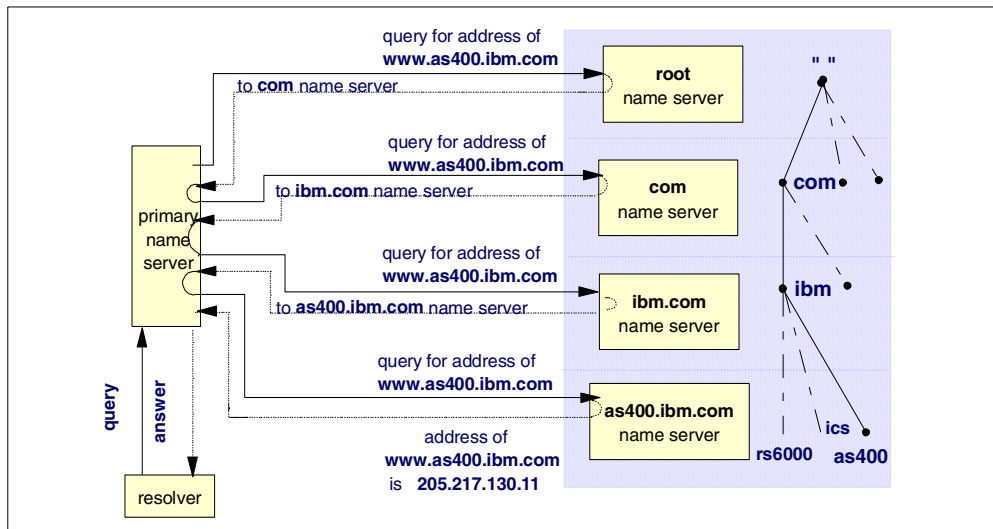


Figure 379. Name resolution example

Recursive versus iterative queries

There are two types of DNS queries: recursive or iterative.

Figure 379 shows an example of one recursive query and several iterative queries. The first query from the resolver to the primary name server is a recursive query. A recursive query requests that, if the name server does not know the answer to the query, it must query other name servers until it finds the answer and then send the answer back to the resolver. Notice in Figure 379, the primary name server did a lot of work. It kept querying other name servers on behalf of the resolver until it could supply the answer. A DNS server is configured to accept recursive queries or only accept iterative queries. The primary name server in Figure 379 was configured to allow recursive queries.

The other name servers queried in Figure 379 (root name server, *com* name server, *ibm.com* name server) were not configured to allow recursive queries. When the primary name server queried the root name server, the query was an

iterative query. This means the root name server responded to the query with the best information it had, which was `I don't know but check the next DNS server: com name server`. The recursive query versus iterative query only comes into play when the name server that was queried does not know the answer to the query. From the example in Figure 379 on page 340, we cannot tell if the `as400.ibm.com` name server is configured to allow recursive queries because this name server held the answer for the primary name server and responded with the answer.

C.5 Types of name servers

There are various types of name servers, which are discussed in the following sections.

Primary name server

This server is where the hosts in the zone of authority are configured. The DNS administrator configures and maintains this server. When this server gives responses to queries from its primary domain files, the responses are called authoritative. A name server for a primary domain reads the primary domain configuration information directly from files configured by the DNS administrator.

Secondary name server

This server has the same information as the primary name server. However, instead of getting its information directly from the DNS administrator configuring it, it gets its information from another name server through zone transfers over the network. The information that a secondary name server obtains from a zone transfer is read into cache as data that is stored from queries.

Note

A DNS server can be a primary name server, as well as a secondary name server, for one or more domains. It can be a name server for primary and secondary domains.

A *zone transfer* is a TCP/IP transfer of domain files from another DNS server (called a *master name server*). This is done automatically when the secondary name server starts and also when the secondary name server detects that its domain files are downlevel from the master name server's domain files. The zone transfer is initiated from the secondary name server. The zone transfer cannot take place if the master name server is not active.

A secondary name server is used for two reasons: spreading the DNS query workload over more than one server and as a backup in case the primary name server stops responding. When a client is configured with more than one DNS server and the first name server (the primary) does not respond, the client can query the second name server (the secondary). When the secondary name server gives a response to a query, the response is also called authoritative. In other words, an answer from a secondary name server is considered to be just as "good" as an answer that came from a primary name server.

Master name server

A master name server is the name server from which a secondary name server gets its zone transfer. A master name server can either be a primary name server or another secondary name server.

Caching-only name server

A name server that does not have authority over any zone is called a *caching-only name server*. It gets all of its information by querying. Caching-only name server responses are always non-authoritative.

Authoritative name server

A server that is considered to be authoritative for a domain is either the primary server for that domain or a secondary server for that domain. *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support, SG24-5147*, shows a scenario that configures a primary and secondary DNS server. If another name server or a client queries either the primary or the secondary name server for information for which they are authoritative, the response is considered to be authoritative. Can a name server that is not authoritative over a domain give a response to a client about that domain and have that response considered an authoritative response? The answer is “yes.” If the non-authoritative server does not know the answer and queries an authoritative name server on behalf of the client and then returns the answer to the client, this response is considered to be authoritative. The non-authoritative name server caches this information. If a second client requests this same information from the non-authoritative name server (and this information is still in its cache), the name server gives the response to the client, but now this same information is labeled non-authoritative. Why? The information in the response this second time came out of the name server’s cache. Another way of saying this is: a non-authoritative response at some point came out of a name server’s cache.

Parent and child name servers

The concept of parent and child domains is equivalent to the concept of a domain and subdomain. Once your domain grows to a certain size, you may need to distribute management by delegating authority of part of your domain to one or multiple subdomains. The upper-level domain is the parent and its subdomains are the children.

The name server authoritative for the parent domain is the parent name server, and the one authoritative for the subdomain is the child name server. For example, in Figure 378 on page 339, *OTHERDOMAIN* is a subdomain of *mycompany.com*. If a DNS server, AS1, is configured to be responsible for the *mycompany.com* zone of authority, and the authority for the zone *OTHERDOMAIN.mycompany.com* is delegated to another DNS server, *OTHERHOST*, then AS1 is considered to be the *parent name server* and *OTHERHOST* is considered to be the *child name server*.

A scenario in which authority is delegated from a parent to a child name server is covered in *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support, SG24-5147*.

Root name servers

Internet root name servers know where name servers authoritative for the top-level domains are. Most of the Internet root name servers are authoritative for the top-level organizational domains (*.com*, *.edu*, *.net*, and so on). The top-level domain servers have information about the second-level domain in which a given domain is located.

A company can implement internal root name servers. In this case, given a query for a company’s subdomain, the internal root name server can provide

information for the second-level subdomain in which the queried subdomain is located.

A root name server is configured in a lower level name server to help it to navigate the name space tree top down when it cannot answer a query with authoritative data or data in its cache.

If we use the example discussed in the previous section, the DNS server *OTHERHOST* is authoritative for the zone *OTHERDOMAIN.mycompany.com* shown in Figure 378 on page 339. AS1 name server is authoritative for the *mycompany.com* zone of authority and is configured as the internal root for the entire company's name space. The internal roots can run on host systems all by themselves or a given host can perform double duty as an internal root and as an authoritative name server for other zones. If *OTHERHOST* cannot answer a query, it asks its root name server, which is AS1 (the DNS server at the top of the *internal* name space tree). We stress *internal* because, in this example, these DNS servers are only part of an internal network. We assume that the network does not have Internet access. Therefore, the Internet "com" node is not part of this DNS name space tree. Therefore, the DNS server AS1 in domain *mycompany.com* is at the top of the tree. A root name server can be thought of as the name server at the *top* of the DNS name space tree. Remember that the DNS name space tree may be different, depending on whether the network is an internal network or if the network includes the Internet DNS name space.

An example of using Internet root name servers is covered in C.4, "Name resolution" on page 339. In this case, the top of the DNS name space tree really was the top of the Internet name space tree, and the root name servers used were the Internet root name servers.

Forwarders

A DNS server can be configured to send the queries, of which it does not know the answer, to a DNS server called a forwarder name server. Where going to a root name server for help in answering a query can be thought of as going to the top of the DNS name space tree, going to a forwarder can be thought of as going side-ways in the DNS name space tree for help. The DNS administrator configures which DNS server is the forwarder. Usually, several DNS servers are configured to have the same forwarder. Then, the forwarder name server is configured with the root name servers (for example, the Internet root name servers). If the forwarders cannot answer the query, they query the root name servers, get the answer, and cache it. This way, a forwarder name server can build up a large cache of information. As the cache increases, chances are that the forwarder will receive a query for which it has a cached answer. This, in turn, reduces the number of times a root name server needs to be queried. Using a forwarder name server is an opportunity to build a large cache of information on one name server (or just a few).

In *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147, we configure an internal DNS server to forward unresolved queries to the company's firewall DNS server.

C.6 Split DNS concept for firewalls

When constructing a firewall, we use Domain Names Services in a particular way so that a company's internal users can locate the IP addresses of all systems (internal and public), while users on the Internet can only locate the IP addresses of the company's public systems. This is part of an effort to hide the company's internal network information from the Internet.

It is not necessary to expose a company's internal network to the Internet. A technique called *split DNS* may be used to only expose the company's public machines to the Internet. Split DNS uses two DNS servers, an internal DNS for secure and private names, and a firewall DNS for the company's "public" names.

The internal DNS server manages the company's internal IP data. The firewall DNS is the only company name server containing information visible from the Internet. Only some of the company's hosts need to be known by the Internet: the e-mail relay, the WWW public server, and the firewall name server itself. The Internet Service Provider (ISP) may provide DNS support for the public hosts in addition to, or instead of, the firewall DNS.

The internal name server forwards queries for information it cannot resolve to the firewall DNS server.

An AS/400 system at release R4V2M0 or above can be a company's internal DNS. Once the AS/400 name server is configured, it contains files of all the company's internal hosts. These files map host names to IP addresses (or vice versa). It does this for a particular domain for which it is responsible (called a zone of authority), for example, the IP address of the host with host name *client1.private.mycompany.com* is *192.168.67.3*. The internal name server lets all of the company's internal hosts locate each other by name in the TCP/IP network.

For protection from the Internet, a company also can use a firewall DNS server. The firewall DNS server's zone of authority is the company's hosts that are public. These are the hosts that the company wants to make visible on the Internet. The split DNS concept is used in the configuration scenario discussed in *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147.

C.7 Primary domain files

These files are configured on the primary name server. On the AS/400 system, they are contained in the IFS directory: */QIBM/UserData/OS400/DNS*. Primary domain files have a *.DB* extension.

Secondary domain backup files

These files contain information that is acquired from zone transfers from the primary name server. They exist on the secondary name server. A secondary name server loads these files and uses them to answer queries, provided the zone transfer was successful.

Forward mapping files

Forward mapping primary domain files reside on the primary name server. They contain all data for mapping host names to IP addresses in a zone. A DNS server is authoritative for a certain part of the DNS name space tree. This part of the tree is called a zone or the DNS server's zone of authority.

Tip

Every forward mapping primary domain file should be configured with the host *localhost* with an IP address of 127.0.0.1.

Reverse mapping files

The reverse mapping primary domain files reside on the primary DNS server. They contain the information for mapping IP addresses to host names in a zone. They are also called the in-addr.arpa files. An example of a reverse mapping file is the *69.5.10.in-addr.arpa* file. A DNS server uses this file if a client resolver queries with an IP address of 10.5.69.222 and asks the DNS server to supply the host name belonging to that IP address. The *69.5.10.in-addr.arpa* file also resides in the AS/400 IFS directory */QIBM/UserData/OS400/DNS* with a file name of *69.5.10.in-addr.arpa.DB*.

Boot file

The boot file is the file the DNS server first reads when it starts. It contains such information as:

- The type of name server
- The zones for which this name server is authoritative
- Where (file location) the name server should get its information

The boot file is also located in the */QIBM/UserData/OS400/DNS* directory.

Note

The presence of the boot file in the IFS directory */QIBM/UserData/OS400/DNS* determines whether the Operations Navigator DNS configuration presents the user with the DNS Wizard windows. If the AS/400 DNS has never been configured, the boot file does not exist. The first time a user clicks on DNS configuration within Operations Navigator, the Wizard windows are presented. Wizard creates the boot file.

Cache file

The cache file contains information about the root name servers. This is where the DNS server should go when it cannot resolve a query itself. This file is located in the */QIBM/UserData/OS400/DNS* directory.

A name server "caches" information it receives from another name server. This is a way a name server "remembers" information so if it receives a query from a client for the same host, it can respond with an answer from its cache and not query the authoritative name server again. It is important to understand that this cached information is *not* contained in the */QIBM/UserData/OS400/DNS/CACHE* file. The *CACHE* file contains information about root servers.

Local file

The local file contains the PTR record for the local loopback interface. The loopback interface, also known as *localhost*, has the IP address of 127.0.0.1. Hosts use the 127.0.0.1 IP address to direct TCP/IP traffic to themselves.

C.8 Types of records

The information contained in forward and reverse primary domain files are organized into records called *resource records*. There are several types of resource records and we try to explain the most common ones in this section. The following list is not a complete list. For more details on resource records, see the second edition of *DNS and BIND* by Albitz & Liu.

A record

Maps a host name to an IP address. There is one A record for every host configured in the DNS server. Consequently, a query that supplies the host name and asks for the IP address is sometimes called an A record query. A records are contained in the forward mapping primary domain file. This type of query is also called a *forward mapping query*.

PTR record

A record that maps an IP address to a host name. There is usually one PTR record for every host configured in the DNS server. These records are located in the reverse mapping primary domain files, which are also called the in-addr.arpa files. A query supplying the IP address and asking for the host name is sometimes called a reverse mapping query, a reverse lookup, or an in-addr.arpa query.

SOA record

The first record in the forward and reverse mapping primary domain files. The SOA record marks the zone of authority in the domain name space. It contains the domain name, the name of the DNS server that is primary for this zone of authority, and the e-mail address of the zone's technical contact. The SOA record also contains the file's serial number. The serial number can be thought of as the change level of the data in this zone. In other words, if a DNS configuration change is made to this zone, the serial number must be incremented (Operations Navigator does this automatically). Also, the SOA record contains refresh timers, retry rates, and expire timers, all having to do with secondary name servers. These terms are further explained in *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147. The SOA record contains the default TTL or time to live. This number controls how long another name server can cache the information supplied out of this name server's zone data. There can be a TTL specified on each resource record, which overrides the TTL specified in the SOA record.

CNAME record

Defines the canonical name of an alias. It is used to specify an alias name for a host.

MX record

Defines a mail exchanger host for a particular domain. This record is used by SMTP to send mail.

NS record

Defines a name server to this name server, either itself or another name server. The other name server can be a name server authoritative over another domain. Or, the other name server can be a secondary name server to this same zone of authority. The NS records allow each name server shown on the right side of Figure 379 on page 340 to tell the primary name server where to query next when it is searching for the

answer to the resolver's query. NS records allow a DNS server to find other DNS servers authoritative for other zones.

C.9 Round robin and address sorting

The concept of round robin and address sorting has to do with how a DNS server responds when it receives an A record query for a host that is multi-homed and has two IP addresses. A multi-homed host is attached to at least two networks. The DNS server always includes both IP addresses in its response. Which IP address is given first depends on the location of the client making the query:

- If the client is physically located in one of the networks in which the host it is querying for is located, the DNS server lists the IP address of that network first in its response. Since clients generally try the IP address that is listed first in the response, this *address sorting* by the DNS server is beneficial because using the host's closer IP address provides better performance.
- If the client is physically located on a network remote to either network in which the host it is querying for is located, the DNS server alternates which IP address it lists first in the response. The next time the name server is queried for the same host from a client that is remote to the host, the other IP address is listed first in the response. This IP address rotation in the DNS server responses is called *round robin*.

A detailed example of round robin and address sorting is discussed in *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147.

C.10 For more information

When a DNS administrator is learning about DNS and how to configure the DNS server on the AS/400 system, we recommend several other resources on DNS that complement this redbook:

- *TCP/IP Configuration and Reference*, SC41-5420
- *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147
- Operations Navigator online help
- *DNS and BIND* by Albitz & Liu
- RFC 1034 (Domain names concepts and facilities), RFC 1035 (Domain names implementations and specifications), and RFC 1912 (Common DNS Operational and Configuration Errors).
- *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162.
- The *comp.protocols.dns.bind* newsgroup located on the Web at:
<http://www.dns.net/dnsrd>

Click on the **Newsgroup** link.

Or, alternatively, go to the Web site at: <http://www.dejanews.com>

Then, issue Search.

Appendix D. Firewall concepts

This appendix provides some basic information about firewalls. It also provides information about using the advanced DNS configuration function of IBM Firewall for AS/400.

D.1 SMTP relay function

The SMTP relay function acts with the following behavior when an SMTP message arrives at the firewall.

D.1.1 Inbound message process

Messages coming from the Internet follow this process:

1. The message arrives on a non-secure port.
2. The SMTP relay replaces the non-secure mail domain name with the secure mail domain name (at the right side of the @ symbol).
3. The SMTP relay asks the firewall DNS to which host this message has to be delivered. The internal SMTP server name is stored as an A record on the DNS.
4. The SMTP relay sends the message to the internal SMTP server.

D.1.2 Outbound message process

Messages going to the Internet follow this process:

1. The message arrives on the Secure port.
2. The SMTP relay replaces the secure mail domain name with the non-secure mail domain name (at the right side of the @ symbol).
3. The SMTP relay asks the ISP DNS to which host this message has to be delivered. It can be any SMTP server or firewall on the Internet.
4. The SMTP relay sends the message to the SMTP server.

D.2 IBM Firewall for AS/400 DNS records created during basic configuration

When you complete the three fields Secure Mail Server, Secure Domain and Public Domain (Figure 380 on page 350) during the basic configuration, the following records are created in the firewall DNS. Several files are created. To find the names of the files, type the following command on the AS/400 command line:

```
SBMNWSCMB CMD ('dir e:/firewall/etc/namedb/*.*') SERVER (FWFS01)
(SVRTYPE(*BASE))
```

Display the job log to view the results.

In this example, we look at the file `named2.dom`. This file contains all the information about the domain `domain1.com`. Similar records are created in the other `.DOM` files for the other domains that are defined.

```

domain1.com          IN  SOA  fw2mail.domain1.com  postmaster...
domain1.com          IN  NS   fw2mail.domain1.com
domain1.com          IN  MX   fw2mail.domain1.com
fw2mail.domain1.com IN  A    208.222.150.250
localhost.domain1.com IN A    127.0.0.1

```



Review Configuration

Review the information that you have entered. Make any changes on this page. When you are sure that the information is correct, print the page for future reference. This creates all the firewall configuration settings. This may take a few minutes to run, so please be patient.

Your AS/400 is: HOME400.SECURE.DOMAIN.COM

Your firewall is: FW2MAIL

Secure domain name servers:

10.100.1.7

Secure Port	IP Address	Subnet Mask
<input checked="" type="radio"/> Port 1	10.100.1.2	255.255.255.0
<input type="radio"/> Port 2	208.222.150.250	255.255.255.248

Secure Mail Server	Secure Domain	Public Domain
domain.com	domain.com	domain.com
domain1.com	domain1.com	domain1.com
domain2.com	domain2.com	domain2.com
domain3.com	domain3.com	domain3.com

Figure 380. Basic firewall configuration summary

D.3 IBM Firewall for AS/400 advanced DNS configuration


People who are familiar with DNS can manually add any type of record in the DNS database interface through the following URL. In this example, `firewall_name` represents the name of the secure port of your firewall:

`http://firewall_name:2001/cgi-bin/db2www/fsdns.mac/main`

The display shown in Figure 381 on page 351 appears.

DNS (Domain Name System) Settings

Public Domain



domain.com
0.0.127.in-addr.arpa

Change Delete Add

Public name servers and IP addresses

Index	Name Server	IP Address
1	dns1.isp.com	194.41.0.4

Index



Change Delete Add

Done

Figure 381. Advanced DNS configuration

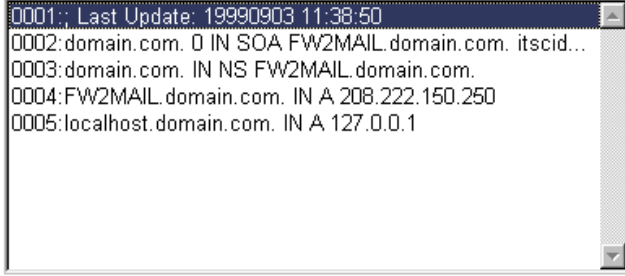
D.3.1 Public domain

This is the domain list of the firewall DNS. In this example, we have one domain, *domain.com*, and one reverse domain, *0.0.127.in-addr.arpa*.

To add, remove, or change records in the DNS database, click the **Change** button. The display shown in Figure 382 on page 352 appears.

Advanced DNS Settings

Select an entry and the option to perform:



0001;	Last Update: 19990903 11:38:50
0002:	domain.com. 0 IN SOA FW2MAIL.domain.com. itscid...
0003:	domain.com. IN NS FW2MAIL.domain.com.
0004:	FW2MAIL.domain.com. IN A 208.222.150.250
0005:	localhost.domain.com. IN A 127.0.0.1

Figure 382. Advanced DNS configuration - Public domain

From the window shown in Figure 382 you can add, remove, and modify any record in the DNS database.

D.3.2 Public name server and IP address

This is the list of public DNS linked with your firewall. Usually the list contains your ISP DNS or the Internet DNS root servers. We strongly recommend that you have at least three DNS in this list.

To add a public DNS in the firewall root server list, click the **Add** button. The display shown in Figure 383 appears.



Name Server	IP Address
dns2.isp.com	128.9.0.107

Figure 383. Public name server

Enter the Name Server fully qualified host name and the IP address.

D.4 Additional firewall information

For more information about IBM Firewall for AS/400, refer to *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162, and *IBM Firewall for AS/400 V4R3: VPN and NAT Support*, SG24-5376. For more information about IBM eNetwork Firewall for Windows NT, refer to *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT*, SG24-5209.

Appendix E. Special notices

This publication is intended to help analysts, consultants, and support people to design, install and configure the e-mail environments. The information in this publication is not intended as the specification of any programming interfaces that are provided by V4R4 of IBM Firewall for AS/400 5769-FW1, V3.3 of IBM eNetwork Firewall for Windows NT, Lotus Domino R4.6.6, or Lotus Domino R5.0.6. See the PUBLICATIONS section of the IBM Programming Announcement for V4R4 of IBM Firewall for AS/400 5769-FW1, V3.3 of IBM eNetwork Firewall for Windows NT, Lotus Domino R4.6.6, and Lotus Domino R5.0.6 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe on any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including, in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating

environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX	AS/400
AT	CT
DB2	DRDA
eNetwork	IBM ®
Net.Data	Netfinity
NetView	OS/400
RS/6000	SecureWay
SP	System/390
XT	400

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere., The Power To Manage., Anything. Anywhere., TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET and the SET logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix F. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

F.1 IBM Redbooks publications

For information on ordering these ITSO publications see “How to get IBM Redbooks” on page 357.

- *AS/400 Internet Security: IBM Firewall for AS/400*, SG24-2162
- *AS/400 - Implementing Windows NT on the Integrated Netfinity Server*, SG24-2164
- *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147
- *Guarding the Gates Using the IBM eNetwork Firewall V3.3 for Windows NT*, SG24-5209
- *IBM Firewall for AS/400 V4R3: VPN and NAT Support*, SG24-5376
- *Lotus Domino for AS/400 R5: Implementation*, SG24-5592

F.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at <http://www.redbooks.ibm.com/> for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbooks Collection	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
Netfinity Hardware and Software Redbooks Collection	SK2T-8046
RS/6000 Redbooks Collection (BkMgr Format)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

F.3 Other resources

These publications are also relevant as further information sources:

- *IBM Firewall for AS/400 Administrator's Guide*, SC41-5419

This book is available in soft copy *only* on the Web at:

<http://www.as400.ibm.com/infocenter>

At the Web site, click **Online library**. Then, select your language and click **Go**. Next, select **V4R4->Category Bookshelves for V4R4->Network Computing and Groupware**. Finally, locate the appropriate title and select it for viewing.

- *Getting Started with IBM Firewall for AS/400*, SC41-5424

- *TCP/IP Configuration and Reference*, SC41-5420
- Albitz, Paul and Liu, Cricket. *DNS and BIND*. O'Reilly & Associates. 1998. ISBN: 1-56-592512-2

F.4 Referenced Web sites

These Web sites are also relevant as further information sources:

- <http://www.as400.ibm.com/infocenter>
Web site where you can obtain *IBM Firewall for AS/400 Administrator's Guide*, SC41-5419, which is available in soft copy only from this site.
- <http://www.redbooks.ibm.com/>
Provides an extensive listing of available redbooks and redbook related information.
- http://www.as400.ibm.com/tstudio/tech_ref/tcp/Indexfr.htm/
Provides information regarding component journaling.
- <http://www.elink.ibm.com/pbl/pbl>
IBM online publications catalog
- <http://www.as400.ibm.com/nt/>
Provides PTF software information and Windows NT Service Pack information.
- <http://www.dns.net/dnsrd/>
By clicking on a Newsgroup link, this site provides access to message board queries originating from the *comp.protocols.dns.bind* newsgroup.
- <http://www.dejanews.com/>
By means of a site Search engine, this site provides access to message board queries originating from the *comp.protocols.dns.bind* newsgroup.
- <http://www.as400.ibm.com/infocenter>
- <http://www.ietf.org>
The Internet Engineering Task Force
- <http://www.as400.ibm.com/vpn>
AS/400 Virtual Private Networking site
- <http://publib.boulder.ibm.com/pubs/pdfs/as400/V4R4PDF/AS4PPCP1.PDF>
- <http://www.icsa.net>
- <http://www.ire.com>
- <http://www.wrs.com>
- <http://publib.boulder.ibm.com/html/as400/infocenter.html>
- <http://as400service.ibm.com>

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** <http://www.redbooks.ibm.com/>

Search for, view, download, or order hardcopy/CD-ROM Redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

Redpieces are Redbooks in progress; not all Redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

Send orders by e-mail including information from the IBM Redbooks fax order form to:

	e-mail address
In United States	usib6fpl@ibmmail.com
Outside North America	Contact information is in the "How to Order" section at this site: http://www.elink.ibm.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the "How to Order" section at this site: http://www.elink.ibm.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the "How to Order" section at this site: http://www.elink.ibm.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the Redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and Redbooks by accessing the IBM Intranet Web site at <http://w3.itso.ibm.com/> and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at <http://w3.ibm.com/> for redbook, residency, and workshop announcements.

IBM Redbooks fax order form

Please send me the following:

Title	Order Number	Quantity
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>
<hr/>	<hr/>	<hr/>

First name

Last name

Company

Address

City

Postal code

Country

Telephone number

Telefax number

VAT number

Invoice to customer number

Credit card number

Credit card expiration date

Card issued to

Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

Symbols

\$oem\$ 309
*LOCAL 122, 184
*SMTPCLT 257
*SMTPSVR 255

Numerics

2852 model (PCI bus) 291
2854 model (PCI bus) 291
2857 model (PCI bus) 291
5769-SS1 (OS/400) 290
5769-TC1 (TCP/IP Utilities) 290
6617 model (SPD bus) 291

A

A record 346, 349
access the POP3 server 37
activating rules 60
Add name for SMTP 68, 70, 128, 129, 172, 174
adding filter rules 37
adding mail domains to the DNS 98
adding new rules 55
adding system names to the DNS 333
adding systems to the domain 23, 97
adding the route entries 333
address sorting 347
administering Domino 78
administrator password 294
alert database 50, 120, 165, 219
alias 275
ALLMAILMSF 265
Allow standard POP connection field 65
Allow standard POP3 connection field 125, 170
AnyMail/MSF dump snap-in 260
AS/400 authorities 292
AS/400 components 2
AS/400 DNS 21, 96, 144, 197
AS/400 DNS to handle the internal domain 22, 96, 198
AS/400 e-mail problem determination 251
AS/400 integration with Windows NT Server 290
AS/400 interface 251
AS/400 NetServer 291
AS/400 planning 289
AS/400 system
 system planning 290
 TCP/IP configuration 304
 virtual token-ring adapter 312
authoritative 338
authoritative name server 342, 343

B

basic configuration 29, 103, 151, 204
Basic FastPath 6
blocking spam
 by domain name 324

 by sender name and domain 325
 by source IP address 326
boot file 345
Bridge Clint 266
Bridge Server 266

C

cache file 345
caching-only name server 342
CD-ROM drive 293
chaining HTTP proxy to another server 327
CHGPOPA 65, 125, 170
CHGSMTPA 265
CHGTCPDMN 122, 123, 168, 184, 185
child and parent name server 342
CNAME record 346
collecting the line trace 261
com 335
communications trace of a line 261
company 13, 14, 139, 193
component journaling 263
configure default route 65
configuring internal DNS to forward queries 201
configuring NAT 33, 34, 51, 53
configuring replications 239
configuring TCP/IP on AS/400 system 304
configuring the internal DNS to forward queries 100, 147
connection 58
connection documents 231
Connections Templates folder 55
connectivity 334
Create Network Address Translation window 35
creating a connection 58
creating a service 56
cross certifying Domino servers 235
current e-mail environment 9
CWBPing 249

D

debugging mail 274
debugging mail on AS/400 system 274
default route 65
delegation 337
disk
 space 296
 storage space 291
disk storage requirements 293
disk storage sizing considerations 294
diskette drive 293
distributed database 335
DNS adding subdomains 24
DNS concepts 335
DNS handling internal domain 22
DNS implementation 335
DNS name explanation 5
DNS name space 336
DNS server 275

- DNS traffic 251
- domain 337
 - adding systems 23
- domain documents 229
- domain file
 - primary 344
 - secondary 344
- domain name system 335, 337
- domain.com 18, 107
- Domino access from the Internet 38, 61
- Domino Administrator on your workstation 74
- Domino e-mail monitoring tools 280
- Domino Message Tracking 253
- Domino server for mail 71, 130, 176
- Domino server for SMTP mail 82, 131, 177, 189, 224
- Domino server on an AS/400 system 71
- Domino server on AS/400 system 175, 221
- Domino server on HOME400 72
- Domino server on MAILSRV2 187
- Domino server on workstation 189
- Domino server with the firewall 85, 134, 180, 227
- Domino with MSF 183
- drive size 294
- dumping Mail Server Framework (MSF) 261

E

- EDTF program 274
- edu 335
- e-mail and virtual IP addresses 334
- e-mail monitoring tools 280
- e-mail problem determination 251
- Ending defense 37
- entry level firewall product 2
- evaluating current e-mail environment 9

F

- file
 - cache 345
 - local 345
- filter rule for Notes access from the Internet 38, 61
- firewall 49, 119, 164, 219, 344
 - network server description 278
 - problem determination 278
- firewall concepts 349
- firewall name to host table entries 64, 124, 169, 186
- forward mapping file 344
- forward queries 26, 100, 147, 201
- forwarder 343
- forwarders to the firewall DNS configuration 326
- FSIOP card 6
- FTP 49, 119, 164, 218
- full domain name 335
- FW1MAIL 27, 28, 29
- FW1NT 39, 40, 52
- FW2MAIL 101, 102, 103
- FW2NT 109
- FW3MAIL 149
- FW3NT 154, 155
- FW4MAIL 202, 203, 204

- FW4NT 208, 209

G

- gov 335

H

- hardware checklist 296
- hardware requirement 1
- HOME400 for handling Domino 72
- HOME400 TCP/IP domain name information 62, 122, 167
- host 64, 124, 169, 186
- host names to the domain 199
- host table entries 64, 124, 169, 186
- HTTP proxy to another server 327

I

- i386 directory 309
- IBM Cryptographic Access Provider 1
- IBM eNetwork Firewall for Windows NT 39, 40, 109, 110, 154, 155, 208, 209, 210, 250
 - DNS implementation 335
- IBM Firewall for AS/400 1, 27, 28, 101, 102, 149, 202, 203, 249
 - advanced DNS configuration 350
 - components 2
 - DNS records created during basic configuration 349
 - positioning 1
 - upgrading 6
 - V4R1 7
 - V4R4 enhancements 3
- inbound mail flow 251
- inbound message process 349
- Incoming Mail Server 275
- installation
 - phase 310
 - Windows NT 305
- installation from the Windows NT console 310
- installation source directory 291
- installation worksheet 297
- installing firewall 61, 65, 122, 125, 167, 169
- installing Windows NT server 307
- INSWNTSVR command 307
- Integrated Netfinity Server pre-installation tasks 303
- Integrated Netfinity Server resource names 292
- interfaces 333
- INTERNAL 64, 124, 249
- internal DNS to forward queries 26
- internal domain 22, 198
- internal LAN addresses 290
- internal root 343
- Internet 37
 - root server 336
- IP address 336, 352
- IP address alias on non-secure LAN 323
- IP address alias on secure LAN 322
- IP forwarding 36
- IP interface 275

- verifying 275
- IPCS card 6
- IPCS hardware 6
- ISP router configuration 33, 52
- iterative 340
- iterative query 340

J

- journal receiver 264, 267
- journaling considerations 266

K

- keyboard 296

L

- LAN adapters 290
- linking Domino servers 228
- local file 345
- Logical Partitioning (LPAR) 292
- Lotus Domino R5 and SMTP configured *MSF 251
- Lotus Domino using native Domino SMTP 253
- Lotus Notes filter rule for access from the Internet 38, 61
- Lotus Notes mail users 86, 135, 181, 192, 246

M

- machine pool size 291
- mail
 - debugging 274
 - routing 336
- mail domains to the DNS 98
- mail environment planning 9
- Mail flow through the Mail Server Framework 252
- mail probes 281
- mail queue 278
- Mail Server Framework 265
- Mail Server journal entries 269
- Mail Service Level parameter 275
- mail tracking 280
- Mail Tracking Collector 283
- mail usage reports 281
- MAILSRV2 184
- MAILSRV2 SMTP server 186
- MAILSRV2 TCP/IP domain name information 184
- MAILSRV2 to handle Domino 187
- MAILSRV3 167, 168, 169
- managing journal receivers 264
- mapping file, forward 344
- mapping files, reverse 345
- mapping POP3 server address 51
- master name server 341
- memory sizing 293
- message tracking on the server 284
- Microsoft Windows NT Server Service Packs 292
- Microsoft Windows NT Service Packs 295
- modes 310
- monitoring mail 253
- mouse 296
- MSF with SMTP domain 185

- MTSTORE.NSF 283
- multiple domain support 3
- multiple domains on a single system 12, 91
- multiple domains on multiple systems 13
- multiple mail servers 4
- multiple SMTP domains on a single AS/400 system 63, 123
- MX record 346
 - removing for domain 107
- MX record for each domain 99, 147
- MX record for each subdomain 25
- MX record for your domain 200
- MXResol 266

N

- name resolution 339
- name server 337, 339
 - authoritative 342
 - caching-only 342
 - forwarder 343
 - master 341
 - parent and child 342
 - primary 341
 - root 342
 - secondary 341
- name server types 341
- NAT 34
 - mapping the POP3 server address 33
- NAT MAP setting syntax 5
- NAT tips 249, 250
- native Domino SMTP 253
- nesting firewalls 326
- netstat 64, 124, 169, 186
- Network Address Translation Settings page 34
- network object 58
- Network Objects 58
- new rules 55
- NS record 346
- nslookup 276

O

- one domain with subdomains on a single system 11, 17
- Online at IPL 319
- OS/400 (5769-SS1) 290
- other firewall functions 321
- outbound mail flow 251
- outbound message process 349

P

- package file 321
- packet filter log messages 4
- pagefile 295
- parameter
 - Mail Service Level 275
 - Preferred address 275
 - search first 275
- parent and child name server 342
- PCI packaging 302

- ping 249, 275
- planning
 - AS/400 system 290
 - considerations for Domino on AS/400 175
 - mail environment 9
 - NAT 51
 - NAT to map the POP3 server address 33
 - Windows NT 293
- POP and SMTP servers 276
- POP mailbox 278
- POP mailbox on AS/400 system 278
- POP3 accounts 66, 67, 126, 170, 171
- POP3 directory entry 275
- POP3 Mail 274
- POP3 mailboxes 70, 130, 174
- POP3 server 71, 130, 175
- POP3 server attributes 65, 125, 170
- POP3 server on the AS/400 MAILSRV3 169
- POP3 server on the AS/400 system 65, 125
- port to Windows NT Server adapter number 316
- post-installation tasks 318
- Preferred address parameter 275
- Pre-V4R4 Flight Recorders 252
- pre-V4R4 SMTP Flight Recorders 253
- preventing spam mail from reaching secure clients 324
- primary domain file 344
- primary name server 340, 341
- problem determination 249
- program temporary fixes (PTFs) 291
- PTFs (program temporary fixes) 291, 292
- PTR record 346
- Public Address Book lookup 244
- public domain 351
- public IP address 33
- public name server 352

Q

- QMSF job 277
- QMSFQUEUE 265
- QSYSWRK subsystem 276
- QTMSINQ 266
- QTMSOUTQ 266
- QTOBDNS job 275
- query
 - iterative 340
 - recursive 340

R

- receive 66
- record
 - CNAME 346
 - file 346
 - MX 346
 - NS 346
 - SOA 346
 - types 346
- recursive 340
- recursive query 340
- registered 51, 52

- relay 349
- removing MX record 107
- replication authority to Domino servers 240
- replications 239, 242
- Reports database for Domino 283
- REPORTS.NSF 283
- requirement
 - hardware 1
 - software 1
- resolver 339
- restart filter 38
- Restore Licensed Program (RSTLICPGM) command 1
- reverse mapping files 345
- root name server 342
- round robin 347
- route entries 333
- route POP3 server responses 65
- router 249
- routing mail 62, 122, 167, 184
- RSTLICPGM (Restore Licensed Program) command 1
- rules 55, 60

S

- scenarios 11
- search first parameter 275
- secondary domain back-up file 344
- secondary name server 341
- Secure Domain 29, 103, 151, 204
- Secure Mail Server 29, 103, 151, 204
- Secure Mail Servers page 108
- server console 293
- service 56, 58
- setting up replications 242
- setting up SMTP attributes 62, 122, 167
- single domain with fanout to multiple systems 14, 193
- SMTP 62, 122, 167, 168, 184, 185
- SMTP and Lotus Domino R5 configured *MSF 251
- SMTP and POP servers 276
- SMTP attributes 62, 122, 167
- SMTP attributes on MAILSRV2 184
- SMTP CInt 266
- SMTP domain 69, 70, 128, 130, 173, 174
- SMTP domain using MSF 185
- SMTP inbound connections 255
- SMTP mail domain on the AS/400 MAILSRV3 168
- SMTP outbound connections 257
- SMTP Outgoing Mail Server 275
- SMTP relay function 349
- SMTP Server 266
- SMTP server 64, 124, 169
- SMTP server on the AS/400 MAILSRV3 167
- SMTP server on the AS/400 system 61, 122
- SMTP system alias table 274
- SMTP traffic 252
- SMTP user ID 69, 70, 128, 130, 173, 174
- SOA record 346
- software checklist 296
- software requirement 1
- spam mail 324
- SPD packaging 301

- split DNS 344
- split DNS concept 344
- Start button improvements 5
- Start Mail Server Framework (STRMSF) command 71, 130, 175
- start NAT 36
- starting the MAILSRV2 SMTP server 186
- starting the POP3 server 71, 130, 175
- starting the SMTP server 124, 169
- STRMSF (Start Mail Server Framework) command 71, 130, 175
- STRMSF command 265, 277
- subdomain 335, 337
- subdomains on a single system 11, 17
- subdomains to the DNS 24
- system distribution directory 67, 126, 171
- system names to the DNS 333
- systems to the domain 97

T

- TCP/IP 290
- TCP/IP configuration 275
- TCP/IP Utilities (5769-TC1) 290
- Telnet 48, 163, 218
- three Domino servers 224
- time synchronization 314
- tracking mail 252
- tracking mail messages 280, 285
- Traffic Control folder 59, 60
- TRCTCPAPP parameter settings for e-mail 255
- trusting the Domino servers 228
- turning on IP forwarding 36

U

- UNATTEND.TXT 309
- unique domain name 336
- upgrade versions of Windows NT Server 294
- upgrading IBM Firewall for AS/400 6

V

- V4R3 enhancement 3
- V4R4 Flight Recorders 252, 255
- viewing the journal receiver 267
- virtual IP address 329
 - and e-mail 334
- virtual LAN 290
- virtual storage file 295
- VPN support 1

W

- Windows NT installation 305
- Windows NT planning 293
- Windows NT Server 290
- Windows NT Server D: and E: drives 294
- Windows NT Server installation 305
- Windows NT Server to support firewalls 289
- Windows NT system 52
- Windows NT virtual storage file 295

- workstation to administer the Domino server 78, 189
- WRKACTJOB SBS(QSYSWRK) command 277
- WRKCFGSTS *NWS command 277
- WRKDIRE 67, 69, 126, 128, 171, 173
- WRKSPLF QMSF command 277

Z

- zone of authority 337
- zone transfer 341

IBM Redbooks evaluation

AS/400 Mail: Multiple SMTP Domains Behind a Firewall
SG24-5643-00

Your feedback is very important to help us maintain the quality of IBM Redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at <http://www.redbooks.ibm.com/>
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Which of the following best describes you?

Customer **Business Partner** **Solution Developer** **IBM employee**
 None of the above

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

What other Redbooks would you like to see published?

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

SG24-5643-00

Printed in the U.S.A.

AS/400 Mail: Multiple SMTP Domains Behind a Firewall

SG24-5643-00

